

# Secure Multiterminal Source Coding with Side Information at the Eavesdropper

Joffrey Villard and Pablo Piantanida

## Abstract

The problem of secure multiterminal source coding with side information at the eavesdropper is investigated. This scenario consists of a main encoder (referred to as Alice) that wishes to compress a single source but simultaneously satisfying the desired requirements on the distortion level at a legitimate receiver (referred to as Bob) and the equivocation rate –average uncertainty– at an eavesdropper (referred to as Eve). It is further assumed the presence of a (public) rate-limited link between Alice and Bob. In this setting, Eve perfectly observes the information bits sent by Alice to Bob and has also access to a correlated source which can be used as side information. A second encoder (referred to as Charlie) helps Bob in estimating Alice's source by sending a compressed version of its own correlated observation via a (private) rate-limited link, which is only observed by Bob. For instance, the problem at hands can be seen as the unification between the Berger-Tung and the secure source coding setups. Inner and outer bounds on the so called rates-distortion-equivocation region are derived. The inner region turns to be tight for two cases: (i) uncoded side information at Bob and (ii) lossless reconstruction of both sources at Bob –secure distributed lossless compression. Application examples to secure lossy source coding of Gaussian and binary sources in the presence of Gaussian and binary/ternary (resp.) side informations are also considered. Optimal coding schemes are characterized for some cases of interest where the statistical differences between the side information at the decoders and the presence of a non-zero distortion at Bob can be fully exploited to guarantee secrecy.

The work of J. Villard is supported by DGA (French Armement Procurement Agency). This research is partially supported by the FP7 Network of Excellence in Wireless COMMUNICATIONS NEWCOM++. The material in this paper was presented in part at the 2010 48th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA; and the 1st International ICST Workshop on Secure Wireless Networks, Cachan, France.

J. Villard and P. Piantanida are with the Department of Telecommunications, SUPELEC, 91192 Gif-sur-Yvette, France (e-mail: joffrey.villard@supelec.fr; pablo.piantanida@supelec.fr).

## I. INTRODUCTION

Consider the classical problem of compressing a source at a sensor node (referred to as Alice) which must be estimated at a remote destination (referred to as Bob) within a certain distortion level. Assume also that a (public) rate-limited link is available between the two devices. In addition to this, the encoder wishes to leak the least possible amount of information about its source to an eavesdropper (referred to as Eve) *e.g.*, an untrusted sensor, who perfectly observes the information bits sent by Alice and may have access to an observation correlated to the source. Another sensor (referred to as Charlie) will help Bob in estimating Alice's source by sending a compressed version of its own correlated observation on a (private) rate-limited link, which is only observed by Bob. In this setting, the correlation between the observations can be useful not only to decrease the rate needed for the communications, but also to increase secrecy, which means the average uncertainty of Eve about Alice's source. From a theoretical viewpoint, the problem at hands is therefore very rich and still quite open, as it contains, as subproblems, the long-standing information-theoretic problem of distributed lossy source coding, as well as recent ones *e.g.*, source coding with security constraints.

Slepian and Wolf [1] introduced the problem of distributed lossless compression *i.e.*, when Bob wants to perfectly estimate both sources of Alice and Charlie. Wyner [2] and Ahlswede and Körner [3] characterized the achievable region when only one source is to be estimated *i.e.*, source coding with coded (or partial) side information. Generalization of the Slepian-Wolf setup to arbitrary distortion levels on both sources was introduced by Berger [4], who provided inner and outer bounds on the achievable region which do not match in general. When Bob is intended to estimate only one source, Berger *et al.* [5] provided a new inner bound which was further proved in [6] to be equivalent to the one of [4], and strictly sub-optimal [7]. Several results of optimality were proved in case of uncoded side information [8], lossless reconstruction of at least one source [9], and in some special cases, including Gaussian sources with quadratic distortion measure [10], [11]. Over the years, these topics have been the focus of intense study and some remarkable progress has been made in theoretical and practical aspects, including general frameworks for lossless compression with multiple terminals [12], [13], lossy source coding with uncertain side information at the decoder [14], [15], lossy compression with partially separated encoders [16] or with many decoders [17]–[19], some results of optimality for Gaussian sources

in various contexts [20], [21], as well as the design of nested codes for distributed compression *e.g.*, using parity-check [22], lattice [22]–[24], or algebraic trellis [25] codes. Nevertheless, in spite of these efforts, the simplest scenario of distributed lossy compression first introduced in [4] still remains open.

On the other hand, extensive research has been done on secure communication. The traditional focus was on cryptography, based on computational complexity where security only depends on the intractability assumption of some hard problems (*e.g.*, factoring large integers). As a matter of fact, the security requirements were only taken into account in the upper layers of the OSI model (*e.g.*, the application layer), assuming that reliable communication/compression schemes were already available. Shannon in [26] introduced the information-theoretic notion of secrecy, where security is measured through the equivocation rate –the remaining uncertainty about the message– at the eavesdropper. This information-theoretic approach of secrecy allows to consider security issues at the physical layer, and ensures unconditionally (regardless of the eavesdropper’s computing power and time) secure schemes, since it only relies on the statistical properties of the system. Adopting this approach in a channel coding perspective, Wyner introduced the wiretap channel in [27] and showed that it is possible to send information at a positive rate with perfect secrecy as long as the channel of the eavesdropper is a degraded version of the legitimate user’s one. Csiszàr and Körner [28] extended this result to the setting of general broadcast channels with any arbitrary equivocation rate. Since then, several extensions have been proposed *e.g.*, for fading channels [29], arbitrary *i.e.*, not necessarily stationary memoryless, channels [30], channels with state information at the encoder [31], cooperative relay broadcast channels [32] (see also [33]–[35] for a review of recent results), as well as practical coding schemes for secure communication *e.g.*, nested codes for (Gaussian and binary) type-II wiretap channels [36], LDPC [37] and lattice [38] codes for the Gaussian wiretap channel, polar codes for binary symmetric channels [39], and construction of secure codes from ordinary channel codes [40]. So far, very few work has been reported on source coding problems with security constraints, while early work [41], [42] showed that the presence of correlation between the different observations may guarantee some secrecy.

Researchers have employed two approaches in the literature of secure source coding. In fact, it is assumed either that there already exists a secure rate-limited link between Alice and Bob, which allows the system to use secret keys, or at least the decoders have access to some side information

about the source. In the scenario of secret key sharing, both lossless and lossy compression have been studied in various contexts [43]–[47]. Classical lossy source coding followed by encryption using the secret key was proved to be optimal when the receivers have no side information [46]. For the second scenario, recent work [48] considered the case of lossless source coding with (uncoded) side information at both decoders under the assumption of no rate constraint in the communication between Alice and Bob. In such a case, the usual Slepian-Wolf scheme is proved to be insufficient. Lossless source coding with coded side information, resp. distributed lossless compression, has been studied in [49], [50], resp. [51]. In their “one-sided helper” scenario, the authors of [50] characterized the achievable region when only one source is to be perfectly estimated and Eve does not have side information. In particular, they proved that the achievable scheme of Wyner [2] and Ahlswede and Körner [3] achieves the whole region. Inner and outer bounds on the achievable region for secure distributed lossless compression have been proposed in [51]. Secure *lossy* source coding with side information at the decoders received less attention. As a matter of fact, if the (uncoded) side informations at the decoders are degraded then the achievable region can be derived as a special case of [47] where Wyner-Ziv coding [8] is optimal.

In this paper, we investigate the general problem of secure lossy source coding of memoryless sources with coded side information at the legitimate receiver in the presence of an eavesdropper, who in addition to observe the information bits can also have access to correlated side information, as depicted in Fig. 1. It is assumed that all links between encoders and decoders are noiseless so that they cannot provide any advantage to increase secrecy. This setting can be seen as the natural extension of the Berger *et al.* problem [5] to the one with security constraints. We provide inner and outer bounds on the achievable region, referred to as the *rates-distortion-equivocation region*. These bounds do not match in general because of a long Markov chain condition, as in [4], [5]. From the proposed inner region, we derive two results of optimality for the cases of: (i) uncoded side information, generalizing the results in [48], [49] to any arbitrary distortion level, and (ii) lossless reconstruction of both sources at the legitimate receiver –distributed lossless compression–, refining [51]. When dealing with the lossy case in the presence of uncoded side information, it should be mentioned here that if one side information (either at Bob or Eve) is less noisy than the other, then Wyner-Ziv coding is sufficient. Similarly, for the distributed lossless compression setting it is shown that if the side information at Eve is less noisy than the observation of Charlie, then Slepian-Wolf coding achieves the whole region. As an application

example, we consider the case of secure lossy source coding of a Gaussian source with Gaussian side informations, extending [10] to the scenario with security constraints. We also consider the case of secure lossy source coding of a binary source, where the (uncoded) side information at Bob (resp. Eve) is the output of a binary erasure channel (resp. a binary symmetric channel) with the source as the input. This model is of theoretical interest since neither Bob nor Eve can always be a lessnoisy decoder.

The rest of this paper is organized as follows. Section II states definitions along with the main results on secure lossy source coding with coded side information at the legitimate receiver. Section III (resp. Section IV) provides an optimal characterization of the achievable region for the case of uncoded side information at Bob (resp. distributed lossless compression). The detailed proofs are relegated to the Appendices as well as a reminder on some useful notions and results. Section V presents application examples to Gaussian and binary sources. Finally, Section VI summarizes the paper and provides discussions.

### Notation

For any sequence  $(x_i)_{i \in \mathbb{N}^*}$ , notation  $x_k^n$  stands for the collection  $(x_k, x_{k+1}, \dots, x_n)$ .  $x_1^n$  is simply denoted by  $x^n$ . Let  $\mathcal{T}$  be an arbitrary finite set. The cardinality of  $\mathcal{T}$  is denoted by  $\|\mathcal{T}\|$ . For any subset  $\mathcal{S} \subset \mathcal{T}$ , notation  $\mathbb{I}_{\mathcal{S}}$  stands for the indicator function of  $\mathcal{S}$  in  $\mathcal{T}$  i.e., for each  $t \in \mathcal{T}$ ,  $\mathbb{I}_{\mathcal{S}}(t) = 1$  if  $t \in \mathcal{S}$ , and  $\mathbb{I}_{\mathcal{S}}(t) = 0$  otherwise. Entropy is denoted by  $H(\cdot)$ , and mutual information by  $I(\cdot; \cdot)$ . We denote typical and conditional typical sets by  $T_{\delta}^n(X)$  and  $T_{\delta}^n(Y|x^n)$ , respectively (see Appendix A-A for details). Let  $X, Y$  and  $Z$  be three random variables on some alphabets with probability distribution  $p$ . If  $p(x|y, z) = p(x|y)$  for each  $x, y, z$ , then  $X, Y$  and  $Z$  form a Markov chain, which is denoted by  $X \dashv Y \dashv Z$ . Random variable  $Y$  is said to be *less noisy* than  $Z$  w.r.t.  $X$  if  $I(U; Y) \geq I(U; Z)$  for each random variable  $U$  such that  $U \dashv X \dashv (Y, Z)$  form a Markov chain. This relation is denoted by  $Y \succeq_X Z$ . For each  $x \in \mathbb{R}$ , notation  $[x]_+$  stands for  $\max(0; x)$ . Logarithms are taken in base 2 and denoted by  $\log(\cdot)$ . For each  $a, b \in [0, 1]$ ,  $a \star b = a(1 - b) + (1 - a)b$ .

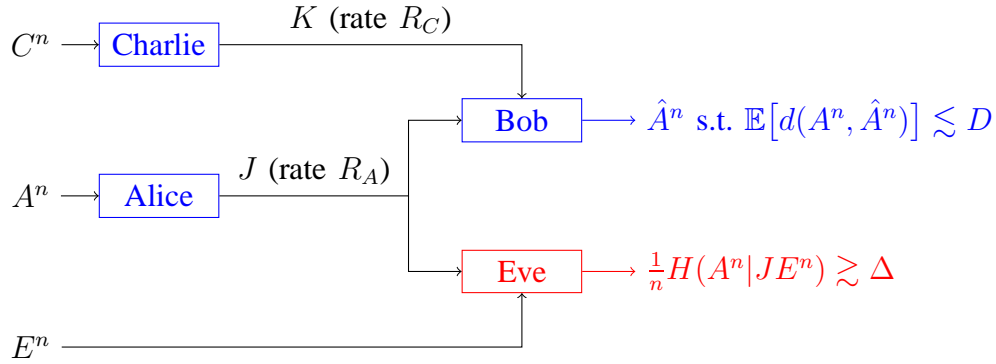


Figure 1: Secure lossy source coding with coded side information.

## II. SECURE LOSSY SOURCE CODING WITH CODED SIDE INFORMATION

### A. Definitions

In this section, we give a more rigorous formulation of the context depicted in Fig. 1. Let  $\mathcal{A}$ ,  $\mathcal{C}$  and  $\mathcal{E}$  be three finite sets. Alice, Charlie and Eve observe sequences of random variables  $(A_i)_{i \in \mathbb{N}^*}$ ,  $(C_i)_{i \in \mathbb{N}^*}$  and  $(E_i)_{i \in \mathbb{N}^*}$  respectively, which take values on  $\mathcal{A}$ ,  $\mathcal{C}$  and  $\mathcal{E}$ , resp. For each  $i \in \mathbb{N}^*$ , random variables  $A_i$ ,  $C_i$  and  $E_i$  are distributed according to the joint distribution  $p(a, c, e)$  on  $\mathcal{A} \times \mathcal{C} \times \mathcal{E}$ . Moreover, they are independent across time  $i$ .

Let  $d : \mathcal{A} \times \mathcal{A} \rightarrow [0; d_{\max}]$  be a finite distortion measure *i.e.*, such that  $0 \leq d_{\max} < \infty$ . We also denote by  $d$  the component-wise mean distortion on  $\mathcal{A}^n \times \mathcal{A}^n$  *i.e.*, for each  $a^n, b^n \in \mathcal{A}^n$ ,  $d(a^n, b^n) \triangleq \frac{1}{n} \sum_{i=1}^n d(a_i, b_i)$ .

*Definition 1:* An  $(n, R_A, R_C)$ -code for source coding in this setup is defined by

- An encoding function at Alice  $f_A : \mathcal{A}^n \rightarrow \{1, \dots, 2^{nR_A}\}$ ,
- An encoding function at Charlie  $f_C : \mathcal{C}^n \rightarrow \{1, \dots, 2^{nR_C}\}$ ,
- A decoding function at Bob  $g : \{1, \dots, 2^{nR_A}\} \times \{1, \dots, 2^{nR_C}\} \rightarrow \mathcal{A}^n$ .

*Definition 2:* A tuple  $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$  is said to be *achievable* if, for any  $\varepsilon > 0$ , there exists an  $(n, R_A + \varepsilon, R_C + \varepsilon)$ -code  $(f_A, f_C, g)$  such that:

$$\begin{aligned} \mathbb{E}[d(A^n, g(f_A(A^n), f_C(C^n)))] &\leq D + \varepsilon, \\ \frac{1}{n} H(A^n | f_A(A^n), E^n) &\geq \Delta - \varepsilon. \end{aligned}$$

The set of all such achievable tuples is denoted by  $\mathcal{R}^*$  and is referred to as the *rates-distortion-equivocation region*.

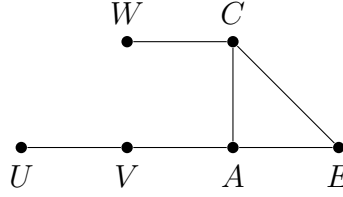


Figure 2: Inner bound—Graphical representation of probability distribution  $p(uvwace)$ .

*Remark 1:* Region  $\mathcal{R}^*$  is closed and convex.

*Remark 2:* Quantities  $\mathbb{E}[d(A^n, g(f_A(A^n), f_C(C^n)))]$  and  $\frac{1}{n} H(A^n | f_A(A^n), E^n)$  in Definition 2 only depend on the marginal distributions  $p(a, c)$  and  $p(a, e)$ , respectively. The same holds for region  $\mathcal{R}^*$ .

### B. Inner and Outer Bounds on the Rates-Distortion-Equivocation Region

The following theorem gives an inner bound on region  $\mathcal{R}^*$  i.e., it defines region  $\mathcal{R}_{\text{in}} \subset \mathcal{R}^*$ .

*Theorem 1:* A tuple  $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$  is achievable if there exist random variables  $U, V, W$  on some finite sets  $\mathcal{U}, \mathcal{V}, \mathcal{W}$ , respectively, s.t. the joint distribution writes  $p(uvwace) = p(u|v)p(v|a)p(w|c)p(ace)$ , and a function  $\hat{A} : \mathcal{V} \times \mathcal{W} \rightarrow \mathcal{A}$ , that verify the following inequalities:

$$R_A \geq I(V; A|W) , \quad (1)$$

$$R_C \geq I(W; C|V) , \quad (2)$$

$$R_A + R_C \geq I(VW; AC) , \quad (3)$$

$$D \geq \mathbb{E}[d(A, \hat{A}(V, W))] , \quad (4)$$

$$\Delta \leq H(A|VW) + I(A; W|U) - I(A; E|U) , \quad (5)$$

$$\Delta - R_C \leq H(A|V) - I(A; E|U) - I(W; C|V) . \quad (6)$$

Region  $\mathcal{R}_{\text{in}}$  is defined as the convex hull of the set of all such tuples.

The proof of Theorem 1 is based on superposition coding and random binning at the encoders Alice and Charlie, and joint decoding at Bob. The proposed scheme along with standard properties of typical sequences enables to characterize the equivocation rate at Eve. The detailed proof is relegated to Appendix B. The above inner region can also be achieved using a time-sharing

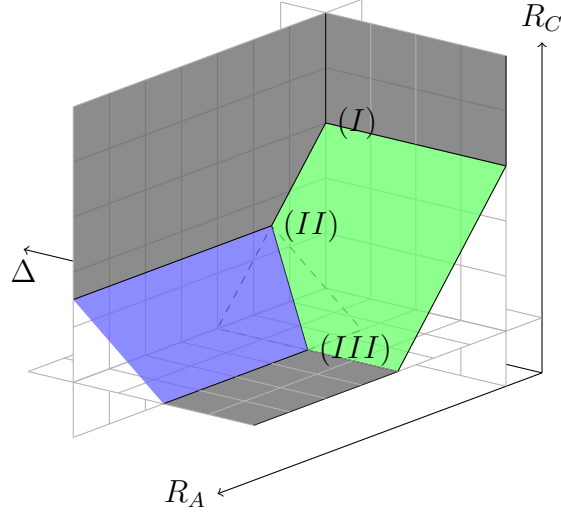


Figure 3: Achievable tuples  $(R_A, R_C, \Delta)$  for some fixed distortion level  $D$ .

combination of three complementary families of codes. Since this approach may yield better intuition, its proof is sketched below.

Inequalities (1)–(3) are identical to the ones of Berger and Tung [4]. They ensure perfect reconstruction of both variables  $V$  and  $W$  at Bob, who can hence compute estimate  $\hat{A}(V, W)$  of  $A$ . The sum-rate constraint (3) captures the trade-off between rates  $R_A$  and  $R_C$ . The information must be transmitted by one or the other encoder.

Let us now give some intuition on Equations (5) and (6). The first term  $H(A|VW)$  corresponds to the equivocation rate at Bob. Alice thus exploits the admissible distortion at Bob to increase the equivocation rate at Eve. Moreover, for given variables  $V$  and  $W$ , which determine the rates and the distortion level at Bob, the auxiliary variable  $U$  can be tuned to make Bob *more capable* than Eve *i.e.*, maximize  $I(A; W|U) - I(A; E|U)$ . This quantity represents the gain (or the loss) at Eve in terms of equivocation rate. At the same time, Equation (6) imposes a trade-off between the equivocation rate at Eve  $\Delta$  and the rate of Charlie  $R_C$ , which captures the fact that  $\Delta$  cannot be too large if  $R_C$  is not. If the secrecy requirement is harsh, more information must be sent through the private link (between Charlie and Bob). We will refer to quantity  $\Delta - R_C$  as the *public-link secrecy rate*.

Note that Equation (5) also writes

$$\Delta \leq H(A|UE) - I(V; A|UW) .$$



Table I: Corner points.

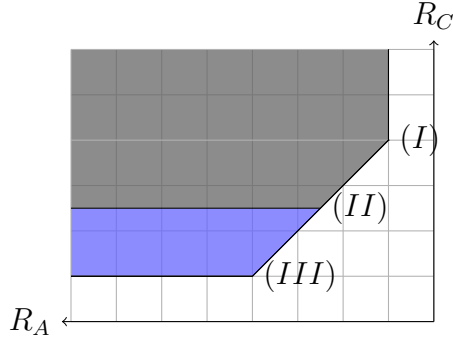
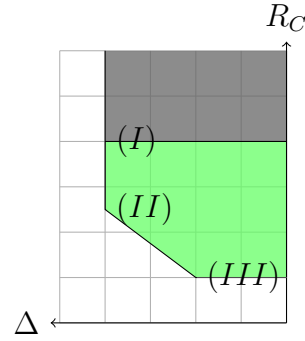
Corner point	(I)	(II)	(III)
Communication order	$W, U, V$	$U, W, V$	$U, V, W$
$R_A$	$I(V; A W)$	$I(U; A) + I(V; A UW)$	$I(V; A)$
$R_C$	$I(W; C)$	$I(W; C U)$	$I(W; C V)$
$D$	$\mathbb{E}[d(A, \hat{A}(V, W))]$	$\mathbb{E}[d(A, \hat{A}(V, W))]$	$\mathbb{E}[d(A, \hat{A}(V, W))]$
$\Delta$	$H(A UE) - I(V; A UW)$	$H(A UE) - I(V; A UW)$	$H(A UE) - I(V; A U)$

Variable  $U$  is thus considered as a *common message* i.e., as if Eve could decode it. As a matter of fact, in case of uncoded side information at Bob (resp. distributed lossless compression), Proposition 3 (resp. 4) shows that it is optimal to encode  $U$  so that Eve can reliably estimate it. The remaining information rate of Alice (on the public link) i.e.,  $I(V; A|UW)$ , is directly subtracted from the equivocation rate, meaning that it is treated as “raw” bits of  $A$ .

*Sketch of proof of Theorem 1 (Time-sharing combination technique):* We first construct three codes achieving corner points (I), (II) and (III) illustrated in Fig. 3, 4 and 5. Each corner point is achieved using a three-step communication scheme which aim is to reliably deliver variables  $(U, V)$  and  $W$ , descriptions of  $A$  at Alice and  $C$  at Charlie, respectively, to Bob. Note that  $V$  is on the top of  $U$  (*superposition coding*). At each step, the information previously received (and decoded) is used as side-information at Bob. *Random binning a la* Wyner-Ziv [8] is performed to take advantage of this side information. These schemes correspond to all possible combinations of the set  $\{U, V, W\}$ , provided that  $U$  is decoded prior to  $V$ , as summarized in row #2 of Table I. For each scheme, the equivocation rate at Eve can be characterized following the argument of Appendix B-H. After Fourier-Motzkin elimination and classical manipulation, we can prove that the three proposed schemes can achieve corner points (I), (II) and (III), which coordinates are given in Table I.

Points (I) and (II) correspond to identical distortion and equivocation rate levels, say  $D$  and  $\Delta$  (see Fig. 5). By a time-sharing combination of these schemes, each point on segment (I)–(II) is also achievable and presents distortion  $D$  and equivocation rate  $\Delta$ . This segment can be easily described since the quantity  $R_A + R_C$  is identical for both points (I) and (II) (see Fig. 4).

Points (II) and (III) correspond to identical distortion level, say  $D$ . By a time-sharing combination of these schemes, each point on segment (II)–(III) is also achievable and presents

Figure 4: Projection on the plane  $\Delta = 0$ .Figure 5: Projection on the plane  $R_A = 0$ .

distortion  $D$ . This segment can be easily described since quantities  $R_A + R_C$  and  $\Delta - R_C$  are identical for both points (II) and (III) (see Fig. 4 and 5, respectively).

Segments (I)–(II) and (II)–(III) define regions which union is delimited by six hyperplanes given by the equations of Theorem 1. ■

*Remark 3:* The simple union of the regions given by the equations of Theorem 1 is not convex. In fact, a time-sharing variable  $T$  cannot be included in auxiliary variables  $U$ ,  $V$  and  $W$ . This would break the long Markov chain  $U \dashv V \dashv A \dashv C \dashv W$  which is essential in our coding scheme.

*Remark 4:* Projections of points (I) and (III) on the plane  $\Delta = 0$  i.e., when there is no secrecy constraint, are those obtained using Berger-Tung coding [4]. In this case, point (II) is useless since it is achievable by a time-sharing combination of points (I) and (III), as shown by Fig. 4. In the general case, the proposed scheme can however improve the security of the transmission, as shown in Fig. 5.

*Remark 5:* When there is no security requirement, Jana and Blahut [6] recently proved the equivalence of the inner bounds of [4] and [5], meaning that point (I) alone yields the same region that points (I) and (III) (after the convex hull operation). A similar result in our secure setting does not seem obvious.

The following proposition gives upper bounds on the cardinalities of alphabets  $\mathcal{U}$ ,  $\mathcal{V}$  and  $\mathcal{W}$ . The proof, which is given in Appendix C, relies on Fenchel-Eggleston-Carathéodory's theorem and follow standard cardinality bounding argument (see [52, Appendix C]).

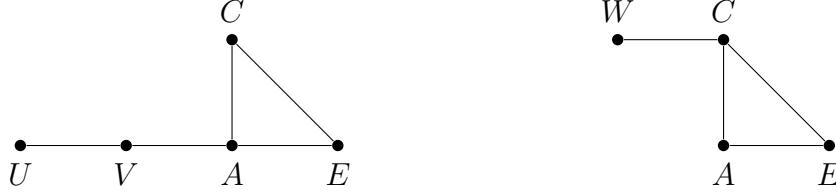


Figure 6: Outer bound—Graphical representation of probability distributions  $p(uvace)$  and  $p(wace)$ .

*Proposition 1:* In the inner region  $\mathcal{R}_{\text{in}}$  given by Theorem 1, it suffices to consider sets  $\mathcal{U}$ ,  $\mathcal{V}$  and  $\mathcal{W}$  such that  $\|\mathcal{U}\| \leq \|\mathcal{A}\| + 5$ ,  $\|\mathcal{V}\| \leq (\|\mathcal{A}\| + 5)(\|\mathcal{A}\| + 3)$  and  $\|\mathcal{W}\| \leq \|\mathcal{C}\| + 3$ .

The following theorem gives an outer bound on region  $\mathcal{R}^*$  i.e., it defines region  $\mathcal{R}_{\text{out}} \supset \mathcal{R}^*$ . The proof is given in Appendix D.

*Theorem 2:* Region  $\mathcal{R}^*$  is included in  $\mathcal{R}_{\text{out}}$ , defined as the closure of the set of all tuples  $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$  such that there exist random variables  $U, V, W$  on some finite sets  $\mathcal{U}, \mathcal{V}, \mathcal{W}$ , respectively, and a function  $\hat{A} : \mathcal{V} \times \mathcal{W} \rightarrow \mathcal{A}$  satisfying  $p(wace) = p(w|c)p(ace)$ ,  $p(uvace) = p(u|v)p(v|a)p(ace)$ , and

$$\begin{aligned}
 R_A &\geq I(V; A|W) , \\
 R_C &\geq I(W; C|V) , \\
 R_A + R_C &\geq I(VW; AC) , \\
 D &\geq \mathbb{E}[d(A, \hat{A}(V, W))] , \\
 \Delta &\leq H(A|VW) + I(A; W|U) - I(A; E|U) , \\
 \Delta - R_C &\leq H(A|V) - I(A; E|U) - I(W; C|V) .
 \end{aligned}$$

As in the classical multiterminal source coding setup [4], the outer region resembles the inner region except that it is convex without time-sharing and that Markov chain conditions  $W \text{---} C \text{---} (A, E)$  and  $U \text{---} V \text{---} A \text{---} (C, E)$  are weaker than the long Markov chain of Theorem 1 (compare Fig. 2 and 6, and see Appendix A-B for details on such graphical representations).

### C. Special Case: Lossless Reconstruction of $A$

In case of lossless reconstruction of  $A$  at Bob,<sup>1</sup> if Eve has no side information ( $E = \emptyset$ ), then point (I) yields the optimal performance choosing auxiliary variables  $U = \emptyset$  and  $V = A$  i.e., using Wyner-Ahlsvede-Körner coding [2], [3], as stated by Tandon *et al.* [50, Theorem 1]: In this case, region  $\mathcal{R}^*$  writes as the closure of the set of all tuples  $(R_A, R_C, D = 0, \Delta) \in \mathbb{R}_+^4$  such that there exists a random variable  $W$  on some finite set  $\mathcal{W}$  s.t.  $W \dashv C \dashv A$  form a Markov chain and

$$R_A \geq H(A|W) ,$$

$$R_C \geq I(W; C) ,$$

$$\Delta \leq I(A; W) .$$

### D. Joint Estimation and Equivocation of Both Sources

Definition 2 only involves the distortion level at Bob and the equivocation rate at Eve about Alice's source. As a matter of fact, the proofs of Theorems 1 and 2 can be used to obtain inner and outer bounds on the achievable region when also considering a distortion constraint on Charlie's source at Bob. This requires the following additional inequality in the definition of the achievability:

$$\mathbb{E}[d_C(C^n, g_C(f_A(A^n), f_C(C^n)))] \leq D_C + \varepsilon ,$$

for some distortion measure  $d_C$  and decoding function  $g_C$ . The resulting bounds will only differ from the ones of Theorems 1 and 2 by adding the following inequality:

$$D_C \geq \mathbb{E}[d_C(C, \hat{C}(V, W))] ,$$

for some function  $\hat{C} : \mathcal{V} \times \mathcal{W} \rightarrow \mathcal{C}$ . For the sake of readability, we did not include this fifth dimension in the main definitions. In Section IV, we remove the distortion, addressing the case of lossless reconstruction of both sources, and prove that region  $\mathcal{R}_{\text{in}}$  yields an optimal characterization of the corresponding achievable region.

Furthermore, the *joint* equivocation rate writes:

$$\frac{1}{n}H(A^n C^n | f_A(A^n), E^n) = \frac{1}{n}H(A^n | f_A(A^n), E^n) + \frac{1}{n}H(C^n | A^n E^n) ,$$

<sup>1</sup>This case is included in the general setup choosing  $d$  as the Kronecker delta and  $D = 0$ .

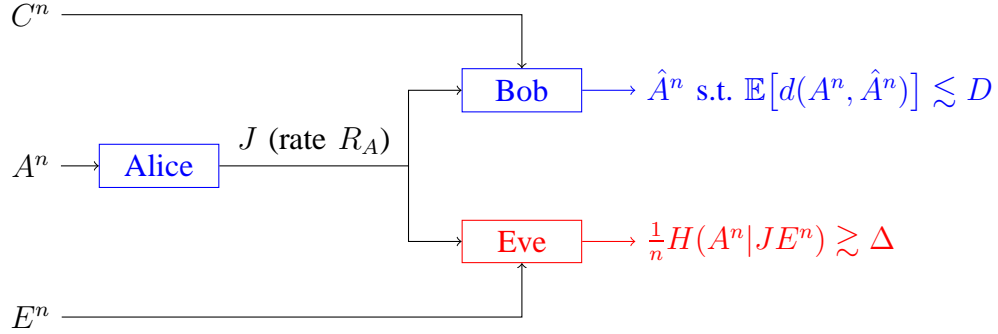


Figure 7: Secure lossy source coding with uncoded side information.

and the last term  $\frac{1}{n}H(C^n | A^n E^n)$  is constant *i.e.*, independent of the coding scheme. Hence, the results involving  $\frac{1}{n}H(A^n | f_A(A^n), E^n)$  directly apply to the joint equivocation rate.

### III. SECURE LOSSY SOURCE CODING WITH UNCODED SIDE INFORMATION

#### A. Definitions

In this section, we consider the special case depicted in Fig. 7 where Bob has access to *uncoded* side information *i.e.*, Bob and Charlie are collocated. We need the following new definitions:

*Definition 3:* An  $(n, R_A)$ -code for source coding in this setup is defined by

- An encoding function at Alice  $f : \mathcal{A}^n \rightarrow \{1, \dots, 2^{nR_A}\}$ ,
- A decoding function at Bob  $g : \{1, \dots, 2^{nR_A}\} \times \mathcal{C}^n \rightarrow \mathcal{A}^n$ .

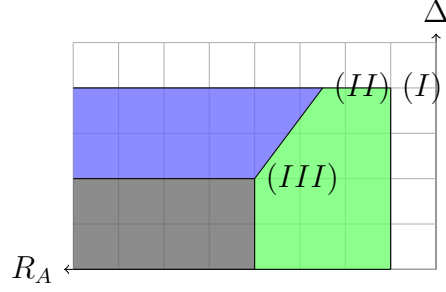
*Definition 4:* A tuple  $(R_A, D, \Delta) \in \mathbb{R}_+^3$  is said to be *achievable* if, for any  $\varepsilon > 0$ , there exists an  $(n, R_A + \varepsilon)$ -code  $(f, g)$  such that:

$$\begin{aligned} \mathbb{E}[d(A^n, g(f(A^n), C^n))] &\leq D + \varepsilon, \\ \frac{1}{n}H(A^n | f(A^n), E^n) &\geq \Delta - \varepsilon. \end{aligned}$$

The set of all such achievable tuples is denoted by  $\mathcal{R}_{\text{uncoded}}^*$  and is referred to as the *rate-distortion-equivocation region*.

#### B. Optimal Characterization

In the setup considered in this section, the following theorem provides a single-letter characterization of region  $\mathcal{R}_{\text{uncoded}}^*$ . The achievability follows from the one of Theorem 1, choosing

Figure 8: Projection on the plane  $R_C = 0$ .

auxiliary variable  $W = C$ , and removing constraints on  $R_C$  (letting  $R_C$  tend to  $\infty$ ) *i.e.*, from the achievability of point (I) (see Fig. 8). A new proof is needed for the converse part (see Appendix E).

Note that if Eve is a legitimate decoder that wishes to estimate source  $A$  within a certain distortion criterion (instead of an eavesdropper that other terminals must contend with), then [19] provides inner and outer bounds on the corresponding rate-distortion function (with two decoders and side-information). Finding an optimal characterization of the achievable region in such a case is still an open problem.

*Theorem 3:* Region  $\mathcal{R}_{\text{uncoded}}^*$  writes as the closure of the set of all tuples  $(R_A, D, \Delta) \in \mathbb{R}_+^3$  such that there exist random variables  $U, V$  on some finite sets  $\mathcal{U}, \mathcal{V}$ , respectively, and a function  $\hat{A} : \mathcal{V} \times \mathcal{C} \rightarrow \mathcal{A}$  such that  $U \dashv V \dashv A \dashv (C, E)$  form a Markov chain and

$$R_A \geq I(V; A|C) , \quad (7)$$

$$D \geq \mathbb{E}[d(A, \hat{A}(V, C))] , \quad (8)$$

$$\Delta \leq H(A|VC) + I(A; C|U) - I(A; E|U) . \quad (9)$$

Comments similar to the ones of Section II-B about Theorem 1 are also relevant here: Equations (7) and (8) are classical in rate-distortion theory, Alice can exploit the admissible distortion at Bob to increase the equivocation rate at Eve (see term  $H(A|VC)$  in Equation (9)), and auxiliary variable  $U$  can be tuned to maximize  $I(A; C|U) - I(A; E|U)$ .

The following proposition gives upper bounds on the cardinalities of alphabets  $\mathcal{U}$  and  $\mathcal{V}$ . The proof is similar to the one of Proposition 1 (given in Appendix C) and is therefore omitted.

*Proposition 2:* In the single-letter characterization of the rate-distortion-equivocation region  $\mathcal{R}_{\text{uncoded}}^*$  given by Theorem 3, it suffices to consider sets  $\mathcal{U}$  and  $\mathcal{V}$  such that  $\|\mathcal{U}\| \leq \|\mathcal{A}\| + 2$  and  $\|\mathcal{V}\| \leq (\|\mathcal{A}\| + 2)(\|\mathcal{A}\| + 1)$ .

### C. Alternative Characterization

The following proposition can be easily proved from Theorem 3.

*Proposition 3:* Region  $\mathcal{R}_{\text{uncoded}}^*$  writes as the closure of the set of all tuples  $(R_A, D, \Delta) \in \mathbb{R}_+^3$  such that there exist random variables  $U, V$  on some finite sets  $\mathcal{U}, \mathcal{V}$ , respectively, and a function  $\hat{A} : \mathcal{V} \times \mathcal{C} \rightarrow \mathcal{A}$  such that  $U \text{---} V \text{---} A \text{---} (C, E)$  form a Markov chain and

$$R_A \geq \left[ I(U; C) - I(U; E) \right]_+ + I(V; A|C) , \quad (10)$$

$$D \geq \mathbb{E}[d(A, \hat{A}(V, C))] , \quad (11)$$

$$\Delta \leq H(A|VC) + I(A; C|U) - I(A; E|U) . \quad (12)$$

*Proof:* Inequalities (10)–(12) yield a smaller region than (7)–(9). The achievability of the above proposition thus follows from the one of Theorem 3.

Notice that the r.h.s. of (9) and (12) writes

$$H(A|VC) + I(A; C) - I(A; E) - \left[ I(U; C) - I(U; E) \right] .$$

Maximizing this term w.r.t.  $U$  thus boils down to minimizing  $I(U; C) - I(U; E)$ . In the worst case, setting  $U = \emptyset$  makes this term zero, meaning that the optimal choice  $U^*$  always leads to  $I(U^*; C) - I(U^*; E) \leq 0$ , and makes Equations (7) and (10) identical. ■

Proposition 3, along with the above proof, indicates that the optimal choice of  $U$  is a random variable  $U^*$  that can be decoded by Eve. Since minimizing quantity  $I(U; C) - I(U; E)$  w.r.t.  $U$  corresponds to looking for a part of  $V$  which conveys more information about  $E$  than  $C$ , this *common message* should however give little information to Eve.

### D. Special Cases of Interest

1) *Lossless secure source coding:* In case of lossless reconstruction of  $A$  at Bob, the following corollary directly follows from Theorem 3.

*Corollary 1:* In case of lossless reconstruction of  $A$  at Bob, region  $\mathcal{R}_{\text{uncoded}}^*$  reduces to the closure of the set of all tuples  $(R_A, D = 0, \Delta) \in \mathbb{R}_+^3$  such that there exists a random variable  $U$  on some finite set  $\mathcal{U}$ , such that  $U \dashv A \dashv (C, E)$  form a Markov chain and

$$\begin{aligned} R_A &\geq H(A|C) , \\ \Delta &\leq I(A; C|U) - I(A; E|U) . \end{aligned}$$

*Remark 6:* In case of a noiseless public link of unlimited capacity *i.e.*,  $R_A \rightarrow \infty$ , the authors of [48] studied the so-called *leakage rate*, defined as  $\liminf \frac{1}{n} I(A^n; JE^n)$ , which equals  $H(A) - \Delta$ . Their result “When Bob remains silent” [48, Theorem 1] thus follows as a special case of Corollary 1.

2) *Bob has less noisy side information than Eve ( $C \succeq_A E$ ):*

*Corollary 2:* If Bob has less noisy side information than Eve, then region  $\mathcal{R}_{\text{uncoded}}^*$  reduces to the closure of the set of all tuples  $(R_A, D, \Delta) \in \mathbb{R}_+^3$  such that there exist a random variable  $V$  on some finite set  $\mathcal{V}$ , and a function  $\hat{A} : \mathcal{V} \times \mathcal{C} \rightarrow \mathcal{A}$  such that  $V \dashv A \dashv (C, E)$  form a Markov chain and

$$\begin{aligned} R_A &\geq I(V; A|C) , \\ D &\geq \mathbb{E}[d(A, \hat{A}(V, C))] , \\ \Delta &\leq H(A|VC) + I(A; C) - I(A; E) . \end{aligned}$$

In this case, random variable  $U$  of Theorem 3 is set to a constant value, and hence Wyner-Ziv coding [8] achieves the whole region.

3) *Eve has less noisy side information than Bob ( $E \succeq_A C$ ):*

*Corollary 3:* If Eve has less noisy side information than Bob, then region  $\mathcal{R}_{\text{uncoded}}^*$  reduces to the closure of the set of all tuples  $(R_A, D, \Delta) \in \mathbb{R}_+^3$  such that there exist a random variable  $V$  on some finite set  $\mathcal{V}$ , and a function  $\hat{A} : \mathcal{V} \times \mathcal{C} \rightarrow \mathcal{A}$  such that  $V \dashv A \dashv (C, E)$  form a Markov chain and

$$\begin{aligned} R_A &\geq I(V; A|C) , \\ D &\geq \mathbb{E}[d(A, \hat{A}(V, C))] , \\ \Delta &\leq H(A|VE) . \end{aligned}$$



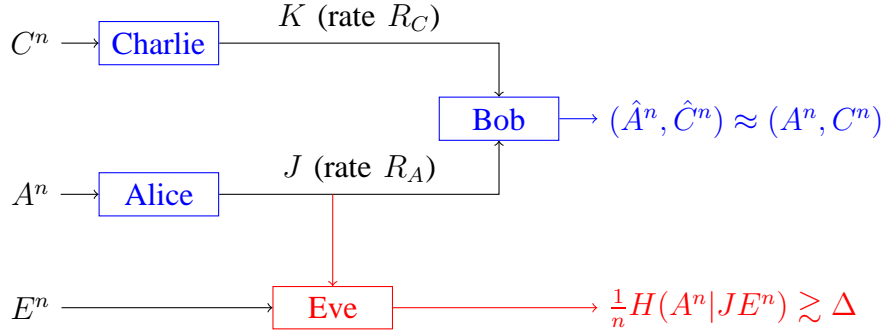


Figure 9: Secure distributed lossless compression.

In this case, random variable  $U$  of Theorem 3 is set to  $V$ , and hence Wyner-Ziv coding [8] achieves the whole region. The equivocation rate at Eve corresponds to the case where Eve can reliably decode  $V$ . Here, Alice can only exploit the available distortion at Bob to achieve a non-zero equivocation rate at Eve.

#### IV. SECURE DISTRIBUTED LOSSLESS COMPRESSION

##### A. Definitions

In this section, we consider the case where Bob wants to perfectly reconstruct both sources  $A$  and  $C$ , from messages  $J$  and  $K$  i.e., *distributed lossless compression*, as depicted in Fig. 9. We need the following new definitions:

*Definition 5:* An  $(n, R_A, R_C)$ -code for distributed compression in this setup is defined by

- An encoding function at Alice  $f_A : \mathcal{A}^n \rightarrow \{1, \dots, 2^{nR_A}\}$ ,
- An encoding function at Charlie  $f_C : \mathcal{C}^n \rightarrow \{1, \dots, 2^{nR_C}\}$ ,
- A decoding function at Bob  $g : \{1, \dots, 2^{nR_A}\} \times \{1, \dots, 2^{nR_C}\} \rightarrow \mathcal{A}^n \times \mathcal{C}^n$ .

*Definition 6:* A tuple  $(R_A, R_C, \Delta) \in \mathbb{R}_+^3$  is said to be *achievable* if, for any  $\varepsilon > 0$ , there exists an  $(n, R_A + \varepsilon, R_C + \varepsilon)$ -code  $(f_A, f_C, g)$  such that:

$$\Pr \{g(f_A(A^n), f_C(C^n)) \neq (A^n, C^n)\} \leq \varepsilon ,$$

$$\frac{1}{n} H(A^n | f_A(A^n), E^n) \geq \Delta - \varepsilon .$$

The set of all such achievable tuples is denoted by  $\mathcal{R}_{\text{lossless}}^*$  and is referred to as the *compression-equivocation rates region*.

### B. Optimal Characterization

In the setup considered in this section, the following theorem provides a single-letter characterization of region  $\mathcal{R}_{\text{lossless}}^*$ . The achievability follows from the one of Points (I) and (II), choosing auxiliary variables  $V = A$  and  $W = C$  (see Section II-B). A new proof is needed for the converse part (see Appendix F).

*Theorem 4:* Region  $\mathcal{R}_{\text{lossless}}^*$  writes as the closure of the set of all tuples  $(R_A, R_C, \Delta) \in \mathbb{R}_+^3$  such that there exists a random variable  $U$  on some finite set  $\mathcal{U}$  verifying the Markov chain  $U \text{---} A \text{---} (C, E)$ , and the following inequalities:

$$R_A \geq H(A|C) , \quad (13)$$

$$R_C \geq H(C|U) , \quad (14)$$

$$R_A + R_C \geq H(AC) , \quad (15)$$

$$\Delta \leq I(A; C|U) - I(A; E|U) . \quad (16)$$

Inequalities (13)–(15) resemble the ones of Slepian and Wolf [1, Section III]. They ensure perfect reconstruction of both variables  $A$  and  $C$  at Bob. Depending on the distribution of  $(A, C, E)$ , variable  $U$  can be tuned to allow non-zero equivocation rate at Eve (see Equation (16)). If the side information at Eve  $E$  is *less noisy* than  $C$  i.e.,  $E \succeq_A C$ , then setting  $U = A$  is optimal, and hence Slepian-Wolf coding achieves the whole region (with  $\Delta = 0$ ).

In case of uncoded side information at Bob, Theorem 4 directly yields Corollary 1 letting  $R_C$  tend to infinity.

*Remark 7:* As a matter of fact, the above result refines recent ones [35], [51] which only provide inner and outer bounds on  $\mathcal{R}_{\text{lossless}}^*$ . It should be mentioned here that the outer bound of [35, Chapter 8], [49], [51] is incorrect. We use [51] as the main reference, but comments below also apply to [35, Chapter 8] and [49] as well. In [51], Equation (5) writes  $\Delta \geq [H(A|E) - R_A]_+$ , meaning that points with  $\Delta = 0$  are not always included in the considered region, while zero equivocation rate is achievable by any coding scheme. This inequality can thus not be proved in the converse part. In fact, Equation (29) is derived using  $H(A^N|E^N, J) \leq \Delta$ , while only the reverse inequality holds.

### C. Alternative Characterization

As in Section III for lossy source coding with uncoded side information, here we can also provide an alternative characterization of region  $\mathcal{R}_{\text{lossless}}^*$ . The achievability follows from the one of Theorem 4. A new proof is needed for the converse part (see Appendix G).

*Proposition 4:* Region  $\mathcal{R}_{\text{lossless}}^*$  writes as the closure of the set of all tuples  $(R_A, R_C, \Delta) \in \mathbb{R}_+^3$  such that there exists a random variable  $U$  on some finite set  $\mathcal{U}$  s.t.  $U \rightarrowtail A \rightarrowtail (C, E)$  form a Markov chain and

$$R_A \geq [I(U; C) - I(U; E)]_+ + H(A|C) , \quad (17)$$

$$R_C \geq H(C|U) , \quad (18)$$

$$R_A + R_C \geq H(AC) , \quad (19)$$

$$\Delta \leq I(A; C|U) - I(A; E|U) . \quad (20)$$

This new single-letter characterization means that *giving  $U$  to Eve is also optimal*. The corresponding additional rate  $[I(U; C) - I(U; E)]_+$  does not lead to a lower equivocation at Eve. This should be considered with reference to known results on the wiretap channel [28], [34], where the so called *common message* can be chosen so that Eve also decodes it, without changing the achievable region.

## V. APPLICATION EXAMPLES

### A. Gaussian Sources with Coded Side Information

Consider the source model depicted in Fig. 10 where the source at Alice is standard Gaussian, and observations at Charlie and Eve are the outputs of independent additive white Gaussian noise (AWGN) channels with input  $A$ , gains  $\rho_C, \rho_E$ , and noise powers  $(1 - \rho_C^2), (1 - \rho_E^2)$ , resp., for some  $0 < \rho_C, \rho_E < 1$ .

Although Theorem 1 is stated and proved for finite alphabet sources, we take the liberty to use its statement, with the appropriate quadratic distortion measure *i.e.*, the Euclidean distance on  $\mathbb{R}$  ( $d(a, b) = (a - b)^2$ , for each  $a, b \in \mathbb{R}$ ), as an achievable region also for Gaussian sources (using differential entropy  $h(\cdot)$ , and considering any equivocation rates  $\Delta \in \mathbb{R}$ ). In this setup, the *rates-distortion-equivocation region* is denoted by  $\mathcal{R}_{\text{Gaussian}}^*$ . Notice that the results should be generalizable to more general cases of continuous-alphabet sources.

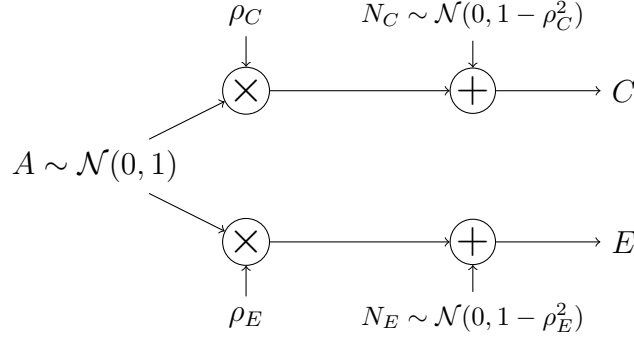


Figure 10: A model for Gaussian sources.

Proposition 5 below provides an inner bound on  $\mathcal{R}_{\text{Gaussian}}^*$  based on the achievability of point (I) (see Section II-B) with Gaussian auxiliary variables. This choice is motivated by [10, Theorem 1] where Oohama proved that it is optimal when only one source is to be estimated within a certain distortion level (with no security constraint).

*Proposition 5:* In the Gaussian setup considered in this section, a tuple  $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^2 \times \mathbb{R}_+^* \times \mathbb{R}$  is achievable if:

$$\begin{aligned}
 R_A &\geq \frac{1}{2} \left[ \log \left( \frac{1 - \rho_C^2 + \rho_C^2 2^{-2R_C}}{D} \right) \right]_+, \\
 \Delta &\leq \frac{1}{2} \log (2\pi e(1 - \rho_E^2)) \\
 &\quad - \frac{1}{2} \min \left\{ \left[ \log \left( \frac{1 - \rho_C^2 + \rho_C^2 2^{-2R_C}}{D} \right) \right]_+ ; \right. \\
 &\quad \left. \log \left( 1 + (1 - \rho_E^2) \left[ \frac{1}{D} - \frac{1}{1 - \rho_C^2 + \rho_C^2 2^{-2R_C}} \right]_+ \right) \right\}.
 \end{aligned}$$

Fig. 11 shows a numerical evaluation of the above inner region setting  $\rho_C = 0.8$ ,  $\rho_E = 0.6$  and  $D = 0.1$ .

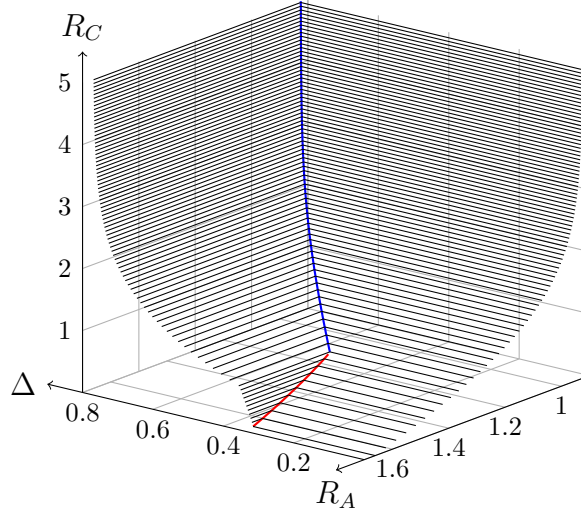


Figure 11: Achievable tuples in the quadratic Gaussian case ( $\rho_C = 0.8$ ,  $\rho_E = 0.6$ ,  $D = 0.1$ ).

*Proof:* Corner point (I) defines a region  $\mathcal{R}_{(I)}$  given by the following inequalities (see Table I in Section II-B):

$$R_A \geq I(V; A|W) , \quad (21)$$

$$R_C \geq I(W; C) , \quad (22)$$

$$D \geq \mathbb{E}[d(A, \hat{A}(V, W))] , \quad (23)$$

$$\Delta \leq h(A|VW) + I(A; W|U) - I(A; E|U) . \quad (24)$$

For some fixed  $R_C \geq 0$  and  $D > 0$ , auxiliary random variables  $U$ ,  $V$  and  $W$  are chosen so that bounds on  $R_A$  and  $\Delta$  given by Proposition 5 yields a point  $(R_A, R_C, D, \Delta)$  in region  $\mathcal{R}_{(I)}$ . More precisely, function  $\hat{A}$  is chosen as the minimum mean square error (MMSE) estimator of  $A$  given  $V$  and  $W$ , and auxiliary variables  $V$  and  $W$  are defined as the outputs of independent AWGN channels with respective inputs  $A$  and  $C$ . The gains of these two channels are tuned to meet constraints (22) and (23), respectively. Then, since variables  $A$ ,  $E$  and  $W$  are Gaussian, either  $W \succeq_A E$ , or  $E \succeq_A W$ . The upper bound (24) is thus maximized setting  $U = \emptyset$ , or  $U = V$ .

1) *Variable  $W$ -Rate at Charlie:* We first define  $\rho_W \in [0, 1)$  by  $\rho_W^2 = 1 - 2^{-2R_C}$ , and choose random variable  $W$  as follows:

$$W = \rho_W C + N_W ,$$

where  $N_W \sim \mathcal{N}(0, 1 - \rho_W^2)$  is an independent random noise. With these definitions,

$$\begin{aligned} I(W; C) &= \frac{1}{2} \log \left( \frac{1}{\text{Var}[C|W]} \right) \\ &= \frac{1}{2} \log \left( \frac{1}{1 - \rho_W^2} \right) \\ &= R_C . \end{aligned}$$

2) *Variable V-Distortion at Bob and Rate at Alice:* We then define  $\rho_V \in [0, 1)$  by

$$\rho_V^2 = \begin{cases} \frac{1 - (\rho_W \rho_C)^2 - D}{1 - (\rho_W \rho_C)^2 - D(\rho_W \rho_C)^2} & \text{if } D < 1 - (\rho_W \rho_C)^2 , \\ 0 & \text{otherwise.} \end{cases} \quad (25)$$

and choose random variable  $V$  as follows:

$$W = \rho_V A + N_V ,$$

where  $N_V \sim \mathcal{N}(0, 1 - \rho_V^2)$  is an independent random noise. Note that if large distortion levels are allowed, then Alice will not transmit anything ( $V = \emptyset$ ).

With these definitions,

$$\begin{aligned} \mathbb{E}[d(A, \hat{A}(V, W))] &= \text{Var}[A|VW] \\ &= \frac{(1 - \rho_V^2)(1 - (\rho_W \rho_C)^2)}{1 - (\rho_V \rho_W \rho_C)^2} \\ &\leq D , \end{aligned}$$

and

$$\begin{aligned} I(V; A|W) &= \frac{1}{2} \log \left( \frac{\text{Var}[A|W]}{\text{Var}[A|VW]} \right) \\ &= \frac{1}{2} \log \left( \frac{1 - (\rho_W \rho_C)^2}{\text{Var}[A|VW]} \right) \\ &= \frac{1}{2} \left[ \log \left( \frac{1 - \rho_C^2 + \rho_C^2 2^{-2R_C}}{D} \right) \right]_+ . \end{aligned}$$

3) *Variable U-Equivocation Rate at Eve:* The above rates and distortion level can be achieved with the following equivocation rate, depending on the choice of  $U$ :

- If  $U = \emptyset$ :

$$\begin{aligned} &h(A|VW) + I(A; W|U) - I(A; E|U) \\ &= h(A|E) - I(V; A|W) \\ &= \frac{1}{2} \log(2\pi e(1 - \rho_E^2)) - \frac{1}{2} \left[ \log \left( \frac{1 - \rho_C^2 + \rho_C^2 2^{-2R_C}}{D} \right) \right]_+ . \end{aligned}$$

- If  $U = V$ :

$$\begin{aligned}
& h(A|VW) + I(A; W|U) - I(A; E|U) \\
&= h(A|E) - I(V; A|E) \\
&= \frac{1}{2} \log(2\pi e(1 - \rho_E^2)) - \frac{1}{2} \log\left(\frac{1 - (\rho_V \rho_E)^2}{1 - \rho_V^2}\right) \\
&= \frac{1}{2} \log(2\pi e(1 - \rho_E^2)) - \frac{1}{2} \log\left(1 + (1 - \rho_E^2) \left[\frac{1}{D} - \frac{1}{1 - \rho_C^2 + \rho_C^2 2^{-2R_C}}\right]_+\right),
\end{aligned}$$

where the last equality follows from definition (25) after some straightforward derivations.

This proves Proposition 5. ■

If Eve has no side information *i.e.*,  $\rho_E = 0$ , then the inner bound given by Proposition 5, and corresponding to Oohama coding [10], is optimal.

*Proposition 6:* If  $\rho_E = 0$ , then region  $\mathcal{R}_{\text{Gaussian}}^*$  reduces to the set of all tuples  $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^2 \times \mathbb{R}_+^* \times \mathbb{R}$  verifying the following inequalities:

$$\begin{aligned}
R_A &\geq \frac{1}{2} \left[ \log\left(\frac{1 - \rho_C^2 + \rho_C^2 2^{-2R_C}}{D}\right) \right]_+, \\
\Delta &\leq \frac{1}{2} \log(2\pi e) - \frac{1}{2} \left[ \log\left(\frac{1 - \rho_C^2 + \rho_C^2 2^{-2R_C}}{D}\right) \right]_+.
\end{aligned}$$

*Proof:* The achievability follows from Proposition 5. The proof of the converse part follows the argument of [10]. Let  $(R_A, R_C, D, \Delta) \in \mathcal{R}_{\text{Gaussian}}^*$  and  $\varepsilon > 0$ . There exists an  $(n, R_A + \varepsilon, R_C + \varepsilon)$ -code  $(f_A, f_C, g)$  s.t.:

$$\begin{aligned}
\mathbb{E}[d(A^n, g(f_A(A^n), f_C(C^n)))] &\leq D + \varepsilon, \\
\frac{1}{n} h(A^n | f_A(A^n), E^n) &= \frac{1}{n} h(A^n | f_A(A^n)) \geq \Delta - \varepsilon.
\end{aligned} \tag{26}$$

Denote by  $J = f_A(A^n)$  and  $K = f_C(C^n)$  the messages transmitted by Alice and Charlie, respectively.

1) *Rate at Alice:* The rate at Alice verifies the following sequence of inequalities:

$$\begin{aligned}
n(R_A + \varepsilon) &\geq H(J) \\
&\geq I(J; A^n | K) \\
&\geq h(A^n | K) - h(A^n | JK).
\end{aligned}$$

We now study each term of the r.h.s. of the above equation. First, note that from the Gaussian distribution of  $(A, C)$  and  $K = f_C(C^n)$ , there exists random variables  $N_{A,i} \sim \mathcal{N}(0, 1 - \rho_C^2)$ ,

independent of  $C^n$  (and hence of  $K$ ) such that  $A_i = \rho_C C_i + N_{A,i}$ , for each  $i \in \{1, \dots, n\}$ . The conditional entropy power inequality (EPI) [52], [53] thus yields

$$\begin{aligned} 2^{\frac{2}{n}h(A^n|K)} &\geq 2^{\frac{2}{n}h(\rho_C C^n|K)} + 2^{\frac{2}{n}h(N_A^n|K)} \\ &= \rho_C^2 2^{\frac{2}{n}h(C^n|K)} + 2\pi e(1 - \rho_C^2) . \end{aligned} \quad (27)$$

On the other hand, the rate at Charlie can be lower bounded as follows:

$$\begin{aligned} n(R_C + \varepsilon) &\geq H(K) \\ &= I(K; C^n) \\ &= h(C^n) - h(C^n|K) . \end{aligned}$$

Equation (27) thus yields

$$\begin{aligned} 2^{\frac{2}{n}h(A^n|K)} &\geq \rho_C^2 2^{\frac{2}{n}(h(C^n) - n(R_C + \varepsilon))} + 2\pi e(1 - \rho_C^2) \\ &= \rho_C^2 2\pi e 2^{-2(R_C + \varepsilon)} + 2\pi e(1 - \rho_C^2) . \end{aligned}$$

Term  $h(A^n|JK)$  can be easily upper bounded:

$$\begin{aligned} h(A^n|JK) &\stackrel{(a)}{=} \sum_{i=1}^n h(A_i|JK A^{i-1}) \\ &\stackrel{(b)}{\leq} \sum_{i=1}^n h(A_i|J, K) \\ &\leq \sum_{i=1}^n \frac{1}{2} \log(2\pi e \text{Var}[A_i|J, K]) \\ &\stackrel{(c)}{\leq} \sum_{i=1}^n \frac{1}{2} \log(2\pi e \mathbb{E}(A_i - g_i(J, K))^2) \\ &\stackrel{(d)}{\leq} \frac{n}{2} \log \left( \frac{2\pi e}{n} \sum_{i=1}^n \mathbb{E}(A_i - g_i(J, K))^2 \right) \\ &\stackrel{(e)}{\leq} \frac{n}{2} \log(2\pi e(D + \varepsilon)) , \end{aligned}$$

where

- step (a) follows from the chain rule for conditional entropy,
- step (b) from the fact that conditioning reduces the entropy,



- step (c) from the fact  $\text{Var}[A_i|J, K]$  is the minimum mean square error (over all possible estimators of  $A_i$ ), for each  $i \in \{1, \dots, n\}$ ,
- step (d) from the fact that function  $\log(\cdot)$  is concave, and Jensen inequality,
- step (e) from the distortion constraint (26).

Putting everything together, we proved that

$$\begin{aligned}
 n(R_A + \varepsilon) &\geq h(A^n|K) - h(A^n|JK) \\
 &\geq \frac{n}{2} \log(\rho_C^2 2\pi e 2^{-2(R_C + \varepsilon)} + 2\pi e(1 - \rho_C^2)) - \frac{n}{2} \log(2\pi e(D + \varepsilon)) \\
 &= \frac{n}{2} \log\left(\frac{1 - \rho_C^2 + \rho_C^2 2^{-2(R_C + \varepsilon)}}{D + \varepsilon}\right).
 \end{aligned}$$

2) *Equivocation Rate at Eve*: The above argument also provides an upper bound on the equivocation rate:

$$\begin{aligned}
 n(\Delta - \varepsilon) &\leq h(A^n) - H(J) \\
 &\leq \frac{n}{2} \log(2\pi e) - \frac{n}{2} \log\left(\frac{1 - \rho_C^2 + \rho_C^2 2^{-2(R_C + \varepsilon)}}{D + \varepsilon}\right).
 \end{aligned}$$

This proves Proposition 6. ■

*Remark 8*: In case of *uncoded* side information at Bob i.e.,  $R_C \rightarrow \infty$ , the inner bound provided by Proposition 5 is optimal if  $\rho_C \geq \rho_E$  i.e.,  $C \succeq_A E$ . The authors conjecture that it also holds if  $\rho_C < \rho_E$ , while the proof seems more tricky.

### B. Binary Source with (Uncoded) BEC/BSC Side Informations

Consider the source model depicted in Fig. 12 where the source is binary and the side information at Bob, resp. Eve, is the output of a binary erasure channel (BEC) with erasure

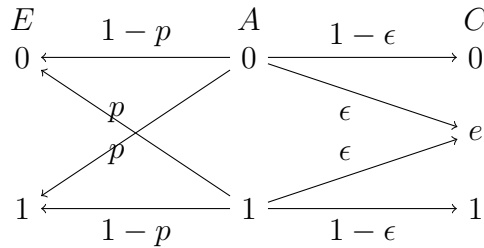
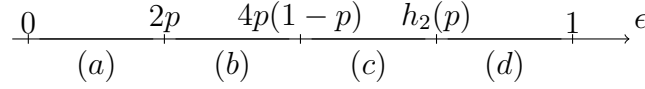


Figure 12: Binary source with BEC/BSC side informations.

Figure 13: The different regions as a function of  $\epsilon$ .

probability  $\epsilon \in [0, 1/2]$ , resp. a binary symmetric channel (BSC) with crossover probability  $p \in [0, 1/2]$ , with input  $A$ .

This model is of interest since neither Bob nor Eve can always be a lessnoisy decoder for all values of  $(p, \epsilon)$ . Let  $h_2$  denote the binary entropy function given by  $h_2(x) = -x \log(x) - (1 - x) \log(1 - x)$ . According to the values of the parameters  $(p, \epsilon)$ , it can be shown by means of standard manipulations [54] that the broadcast channel with input  $A$  and outputs  $(C, E)$  satisfies the following properties (see Fig. 13):

- (a)  $0 \leq \epsilon \leq 2p$ : The side information  $E$  is a stochastically degraded version of  $C$ ,
- (b)  $2p \leq \epsilon \leq 4p(1 - p)$ : The side information  $C$  is less noisy than  $E$  i.e.,  $C \succeq_A E$ ,
- (c)  $4p(1 - p) \leq \epsilon \leq h_2(p)$ : The side information  $C$  is more capable than  $E$ , i.e.,  $I(A; C) \geq I(A; E)$ ,
- (d)  $h_2(p) < \epsilon \leq 1$ : Any of the above relations hold between the side informations  $C$  and  $E$ .

Corollary 2 thus provides an optimal characterization of the rate-distortion-equivocation region  $\mathcal{R}_{\text{uncoded}}^*$  when  $\epsilon$  lies in region (a) or (b). Otherwise, only Theorem 3 applies for the general case and variable  $U$  is neither constant nor equal to  $V$ .

From now on, let the distortion function at Bob  $d$  be the Hamming distance and assume for simplicity that the source is uniformly distributed, i.e.,  $\Pr\{A = 0\} = \Pr\{A = 1\} = 1/2$ . We know from the cardinality constraints given in Proposition 2 that it suffices to consider sets  $\mathcal{U}$  and  $\mathcal{V}$  such that  $\|\mathcal{U}\| \leq 4$  and  $\|\mathcal{V}\| \leq 12$ . As a matter of fact, according to the following proposition, we can restrict our attention to the auxiliary variables  $(U, V)$  obtained as the outputs of a degraded binary symmetric broadcast channel with input  $A$ , as depicted in Fig. 14. Notice that  $V$  is identical to the auxiliary variable used by Wyner and Ziv [8] for the rate-distortion function of a binary source in the case where there is no eavesdropper.

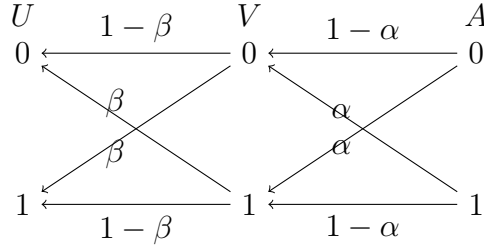


Figure 14: Binary auxiliary random variables.

*Proposition 7:* In the case considered in this section, region  $\mathcal{R}_{\text{uncoded}}^*$  reduces to the set of all tuples  $(R_A, D, \Delta) \in \mathbb{R}_+^3$  such that there exist  $\alpha, \beta \in [0, 1/2]$  satisfying

$$R_A \geq \epsilon (1 - h_2(\alpha)) ,$$

$$D \geq \epsilon \alpha ,$$

$$\Delta \leq \epsilon h_2(\alpha) + (1 - \epsilon) h_2(\alpha \star \beta) - h_2(p \star \alpha \star \beta) + h_2(p) .$$

*Proof:* The achievability part of Proposition 7 is a direct application of Theorem 3: define auxiliary random variables  $U$  and  $V$  as depicted in Fig. 14, and function  $\hat{A}$  on  $\mathcal{V} \times \mathcal{C} = \{0, 1\} \times \{0, e, 1\}$  by

$$\hat{A}(v, c) = \begin{cases} c & \text{if } c \neq e , \\ v & \text{otherwise} . \end{cases}$$

Expressions of Proposition 7 follow after some straightforward derivations.

The converse part needs more arguments. Let  $(R_A, D, \Delta)$  be an achievable tuple. From Theorem 3, there exist finite sets  $\mathcal{U}, \mathcal{V}$ , random variables  $U$  on  $\mathcal{U}$ ,  $V$  on  $\mathcal{V}$  and a function  $\hat{A} : \mathcal{V} \rightarrow \mathcal{A}$ , s.t.  $U \text{ --- } V \text{ --- } A \text{ --- } (C, E)$  form a Markov chain and

$$R_A \geq \epsilon I(V; A) ,$$

$$D \geq \epsilon \mathbb{E}[d(A, \hat{A}(V))] ,$$

$$\Delta \leq \epsilon H(A|V) + (1 - \epsilon) H(A|U) - H(E|U) + h_2(p) .$$

The proof of the above expressions is straightforward, and hence it is omitted here. We now prove that there exist  $\alpha, \beta \in [0, 1/2]$  satisfying the inequalities of Proposition 7:

1) *Rate*: Random variable  $A$  is uniformly distributed on  $\{0, 1\}$ , thus:

$$\begin{aligned} I(V; A) &= H(A) - H(A|V) \\ &= 1 - H(A|V) . \end{aligned}$$

Since  $0 \leq H(A|V) \leq H(A) = 1$ , and function  $h_2$  is a continuous one-to-one mapping from  $[0, 1/2]$  to  $[0, 1]$ , there exists  $\alpha \in [0, 1/2]$  such that  $H(A|V) = h_2(\alpha)$ , and

$$I(V; A) = 1 - h_2(\alpha) .$$

2) *Distortion at Bob*: Since distortion  $d$  is the Hamming distance, we can write:

$$\mathbb{E}[d(A, \hat{A}(V))] = \Pr \left\{ \hat{A}(V) \neq A \right\} ,$$

and, from Fano's inequality [53]:

$$h_2 \left( \Pr \left\{ \hat{A}(V) \neq A \right\} \right) + \Pr \left\{ \hat{A}(V) \neq A \right\} \log(\|\mathcal{A}\| - 1) \geq H(A|V) ,$$

i.e.,

$$h_2 \left( \Pr \left\{ \hat{A}(V) \neq A \right\} \right) \geq h_2(\alpha) .$$

Function  $h_2$  is increasing on  $[0, 1/2]$ , and  $\alpha \in [0, 1/2]$ . The last inequality thus implies

$$\Pr \left\{ \hat{A}(V) \neq A \right\} \geq \alpha .$$

3) *Equivocation Rate at Eve*: Define r.v.  $\hat{V}$  on  $\{0, 1\}$  as the output of a BSC with crossover probability  $\alpha$  and input  $A$ . Since  $A$  is uniformly distributed on  $\{0, 1\}$ ,  $A$  is also the output of a BSC with crossover probability  $\alpha$  and input  $\hat{V}$ . From Mrs. Gerber's lemma [55], we can write, for each  $u \in \mathcal{U}$ :

$$H(A|U = u) = h_2 \left( \alpha \star h_2^{-1}(H(\hat{V}|U = u)) \right) ,$$

and hence,

$$H(A|U) = \sum_{u \in \mathcal{U}} h_2 \left( \alpha \star h_2^{-1}(H(\hat{V}|U = u)) \right) p(u) .$$

Following the same argument, since  $E$  is the output of a BSC with crossover probability  $p$  and input  $A$ , it is also the output of a BSC with crossover probability  $p \star \alpha$  and input  $\hat{V}$ , and:

$$H(E|U) = \sum_{u \in \mathcal{U}} h_2 \left( (p \star \alpha) \star h_2^{-1}(H(\hat{V}|U = u)) \right) p(u) .$$

Now, for each  $u \in \mathcal{U}$ ,  $0 \leq H(\hat{V}|U = u) \leq H(\hat{V}) \leq 1$ , and there exists  $\beta_u \in [0, 1/2]$  such that  $H(\hat{V}|U = u) = h_2(\beta_u)$ . Consequently,

$$\begin{aligned} (1 - \epsilon)H(A|U) - H(E|U) &= \sum_{u \in \mathcal{U}} \left[ (1 - \epsilon) h_2(\alpha \star \beta_u) - h_2(p \star \alpha \star \beta_u) \right] p(u) \\ &\leq (1 - \epsilon) h_2(\alpha \star \beta) - h_2(p \star \alpha \star \beta) , \end{aligned}$$

where  $\beta = \beta_{u^*}$  for some  $u^* \in \mathcal{U}$ .

This proves Proposition 7. ■

*Remark 9:* In this binary case with Hamming distance as distortion measure, an achievable distortion level  $D$  is an upper bound on the average bit error rate (BER) at Bob (while estimating  $A$ ):

$$\mathbb{E}[d(A^n, g(f(A^n), C^n))] = \frac{1}{n} \sum_{i=1}^n \Pr \{ \hat{A}_i \neq A_i \} ,$$

where  $\hat{A}_i \triangleq g_i(f_A(A^n), C^n)$  is the  $i$ -th coordinate of the estimate of  $A^n$  at Bob. At the same time, an achievable equivocation rate  $\Delta$  provides a lower bound on the BER at Eve, as shown by the following sequence of inequalities:

$$\begin{aligned} \frac{1}{n} H(A^n | JE^n) &\stackrel{(a)}{\leq} \frac{1}{n} H(A^n | \check{A}^n) \\ &\stackrel{(b)}{\leq} \frac{1}{n} \sum_{i=1}^n H(A_i | \check{A}_i) \\ &\stackrel{(c)}{=} \frac{1}{n} \sum_{i=1}^n H(W_i | \check{A}_i) + H(A_i | W_i \check{A}_i) \\ &\stackrel{(d)}{\leq} \frac{1}{n} \sum_{i=1}^n H(W_i) \\ &= \frac{1}{n} \sum_{i=1}^n h_2 \left( \Pr \{ \check{A}_i \neq A_i \} \right) \\ &\stackrel{(e)}{\leq} h_2 \left( \frac{1}{n} \sum_{i=1}^n \Pr \{ \check{A}_i \neq A_i \} \right) , \end{aligned}$$

where

- step (a) holds for any  $\check{A}^n \in \mathcal{A}^n$  such that  $\check{A}^n \text{---} (J, E^n) \text{---} A^n$  form a Markov chain,
- step (b) follows from the chain rule for conditional entropy and the fact that conditioning reduces the entropy,
- step (c) from  $W_i \triangleq A_i \oplus \check{A}_i$ , for each  $i \in \{1, \dots, n\}$ ,

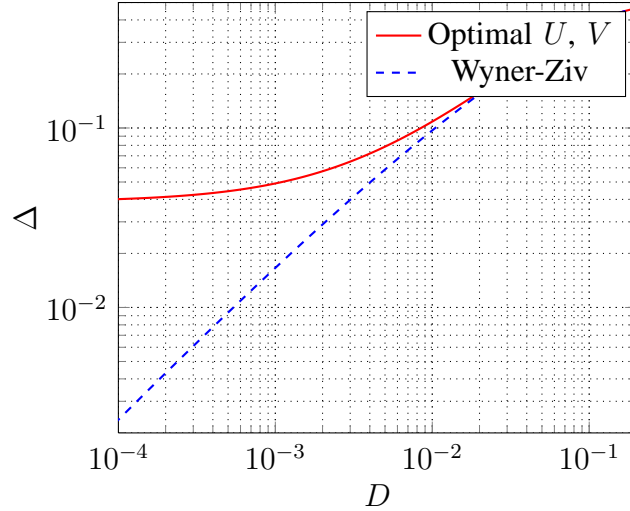


Figure 15: Equivocation rate at Eve as a function of the distortion level at Bob ( $p = 0.1$ ,  $\epsilon = h_2(p) \approx 0.469$ ).

- step (d) from identity  $A_i = W_i \oplus \check{A}_i$  and the fact that conditioning reduces the entropy,
- step (e) from the fact that function  $h_2$  is concave, and Jensen inequality.

*Numerical evaluation:* Using the inequalities of Proposition 7, we now numerically compute some achievable tuples for  $p = 0.1$  and  $\epsilon = h_2(p) \approx 0.469$  (see Fig. 15). In case of lossless compression (columns #1 and #2 of Table II), the auxiliary random variable  $V$  is set to  $A$  i.e.,  $\alpha = 0$ . Variable  $U$  actually enables a non-zero equivocation level. Now assume that the coding rate is limited to a maximum of 80% of the required rate for perfect reconstruction of the source (column #3). This induces a distortion of 0.015 at Bob and an equivocation rate of 0.133 bits at

Table II: Some achievable tuples and corresponding parameters for auxiliary random variables ( $p = 0.1$ ,  $\epsilon = h_2(p) \approx 0.469$ ).

	Secure source coding	Slepian-Wolf	Secure source coding	Wyner-Ziv
Rate $R$	0.469	0.469	0.375	0.375
Distortion $D$	0	0	0.015	0.015
Equivocation Rate $\Delta$	0.039	0	0.133	0.126
$\alpha$	0	0	0.031	0.031
$\beta$	0.078	0	0.050	0

Eve. Even a small increase in the distortion at Bob can be fully exploited by Alice to achieve very significant gains (more than third times in this case) in terms of equivocation rate at Eve. Moreover, for distortion levels higher than 0.036, Wyner-Ziv coding actually achieves the optimal performance, as shown in Fig. 15.

## VI. SUMMARY AND DISCUSSIONS

In this paper, we have addressed the general problem of secure lossy source coding with coded side information. Inner and outer bounds on the corresponding achievable region have been derived. This setting can be seen as the natural extension of the Berger *et al.* problem [5] by taking the security requirements into account. It should be mentioned here that the latter is a fundamental information-theoretic problem for which the best known inner bound is not optimal in general. In the same way, our proposed bounds do not match in general, but the achievable inner region turns to be optimal for two cases of particular interest. Namely, secure lossy source coding with uncoded side information, and secure distributed lossless compression. Interestingly enough, it is proved for both cases that there is no loss in coding to provide a *common* description of the source to both receivers, the legitimate one and the eavesdropper. The remaining information is intended to the legitimate receiver and considered at the eavesdropper as “raw” bits. Furthermore, under certain conditions (*e.g.*, *less noisy*), the standalone Wyner-Ziv (or Slepian-Wolf) coding scheme can achieve the entire region and hence the highest security is guaranteed without additional efforts.

Application examples to secure lossy source coding of Gaussian and binary sources have been considered. The binary model is of interest since neither Bob nor Eve can always be a lessnoisy decoder and thus the encoding strategy needed to achieve the whole region is rather novel. In the Gaussian quadratic case, the results by Oohama [10] suggest an inner bound which has been proved to be optimal in some cases. A deep analysis along with recent extremal inequalities [56], [57] may yield the expected converse. However, in the light of known results on Gaussian quadratic multiterminal compression [10], [11], [20], [21], [58], this might be a tricky problem.

Several possible extensions of this work can be identified. First of all, we can think about an extension of the CEO problem [59], [60] under some security constraints, where the purpose of the legitimate decoder is to estimate a common underlying random variable. Recent results [61]

indicate that Wyner-Ziv-like coding works well in this setup, and the quadratic Gaussian case has already been solved by Oohama [62]. Since the quantity of interest is the underlying variable, the secrecy of the system could be measured by the equivocation at the eavesdropper about this variable rather than the observation of one encoder.

Further extensions could include the introduction of multiple eavesdroppers in order to consider the fact that the encoder cannot reliably know the statistics of the information at the eavesdropper. As a matter of fact, if the observations of these multiple eavesdroppers are degraded (or maybe less noisy), as it will be the case with scalar Gaussian variables, then a multi-layer superposition coding scheme may yield a characterization of the equivocation rate at each eavesdropper.

Through this work, error-free rate-limited links were assumed between the encoders and receivers, while noisy channels could provide additional security, as in the traditional wiretap setting. A result of optimality for the case of degraded channels and side informations has already been derived [47]. A comprehensive study of the more general setup of *secure joint source/channel coding* seems promising.



## APPENDIX A

### USEFUL NOTIONS AND RESULTS

The appendices below provide basic notions on some concepts used in this paper.

#### A. Strongly Typical Sequences and Delta-Convention

Following [63], we use in this paper *strongly typical sets* and the so-called *Delta-Convention*. Some useful facts are recalled here. Let  $X$  and  $Y$  be random variables on some finite sets  $\mathcal{X}$  and  $\mathcal{Y}$ , respectively. We denote by  $P_{X,Y}$  (resp.  $P_{Y|X}$ , and  $P_X$ ) the joint probability distribution of  $(X, Y)$  (resp. conditional distribution of  $Y$  given  $X$ , and marginal distribution of  $X$ ).

*Definition 7:* For any sequence  $x^n \in \mathcal{X}^n$  and any symbol  $a \in \mathcal{X}$ , notation  $N(a|x^n)$  stands for the number of occurrences of  $a$  in  $x^n$ .

*Definition 8:* A sequence  $x^n \in \mathcal{X}^n$  is called (*strongly*)  $\delta$ -*typical* w.r.t.  $X$  (or simply *typical* if the context is clear) if

$$\left| \frac{1}{n} N(a|x^n) - P_X(a) \right| \leq \delta \quad \text{for each } a \in \mathcal{X} ,$$

and  $N(a|x^n) = 0$  for each  $a \in \mathcal{X}$  such that  $P_X(a) = 0$ . The set of all such sequences is denoted by  $T_\delta^n(X)$ .

*Definition 9:* Let  $x^n \in \mathcal{X}^n$ . A sequence  $y^n \in \mathcal{Y}^n$  is called (*strongly*)  $\delta$ -*typical* (w.r.t.  $Y$ ) given  $x^n$  if

$$\left| \frac{1}{n} N(a, b|x^n, y^n) - \frac{1}{n} N(a|x^n) P_{Y|X}(b|a) \right| \leq \delta \quad \text{for each } a \in \mathcal{X}, b \in \mathcal{Y} ,$$

and,  $N(a, b|x^n, y^n) = 0$  for each  $a \in \mathcal{X}$ ,  $b \in \mathcal{Y}$  such that  $P_{Y|X}(b|a) = 0$ . The set of all such sequences is denoted by  $T_\delta^n(Y|x^n)$ .

*Delta-Convention* [63]: For any sets  $\mathcal{X}$ ,  $\mathcal{Y}$ , there exists a sequence  $\{\delta_n\}_{n \in \mathbb{N}^*}$  such that lemmas below hold.<sup>2</sup> From now on, typical sequences are understood with  $\delta = \delta_n$ . Typical sets are still denoted by  $T_\delta^n(\cdot)$ .

*Lemma 1* ( [63, Lemma 1.2.12]): There exists a sequence  $\eta_n \xrightarrow[n \rightarrow \infty]{} 0$  such that

$$P_X(T_\delta^n(X)) \geq 1 - \eta_n .$$

<sup>2</sup>As a matter of fact,  $\delta_n \rightarrow 0$  and  $\sqrt{n} \delta_n \rightarrow \infty$  as  $n \rightarrow \infty$ .

*Lemma 2* ([63, Lemma 1.2.13]): There exists a sequence  $\eta_n \xrightarrow{n \rightarrow \infty} 0$  such that, for each  $x^n \in T_\delta^n(X)$ ,

$$\left| \frac{1}{n} \log \|T_\delta^n(X)\| - H(X) \right| \leq \eta_n ,$$

$$\left| \frac{1}{n} \log \|T_\delta^n(Y|x^n)\| - H(Y|X) \right| \leq \eta_n .$$

*Lemma 3* (Asymptotic equipartition property): There exists a sequence  $\eta_n \xrightarrow{n \rightarrow \infty} 0$  such that, for each  $x^n \in T_\delta^n(X)$  and each  $y^n \in T_\delta^n(Y|x^n)$ ,

$$\left| -\frac{1}{n} \log P_X(x^n) - H(X) \right| \leq \eta_n ,$$

$$\left| -\frac{1}{n} \log P_{Y|X}(y^n|x^n) - H(Y|X) \right| \leq \eta_n .$$

*Lemma 4* (Joint typicality lemma [52]): There exists a sequence  $\eta_n \xrightarrow{n \rightarrow \infty} 0$  such that

$$\left| -\frac{1}{n} \log P_Y(T_\delta^n(Y|x^n)) - I(X; Y) \right| \leq \eta_n \text{ for each } x^n \in T_\delta^n(X) .$$

*Proof:*

$$\begin{aligned} P_Y(T_\delta^n(Y|x^n)) &= \sum_{y^n \in T_\delta^n(Y|x^n)} P_Y(y^n) \\ &\stackrel{(a)}{\leq} \|T_\delta^n(Y|x^n)\| 2^{-n[H(Y)-\alpha_n]} \\ &\stackrel{(b)}{\leq} 2^{n[H(Y|X)+\beta_n]} 2^{-n[H(Y)-\alpha_n]} \\ &= 2^{-n[I(X;Y)-\beta_n-\alpha_n]} , \end{aligned}$$

where

- step (a) follows from the fact that  $T_\delta^n(Y|x^n) \subset T_\delta^n(Y)$  and Lemma 3, for some sequence

$$\alpha_n \xrightarrow{n \rightarrow \infty} 0 ,$$

- step (b) from Lemma 2, for some sequence  $\beta_n \xrightarrow{n \rightarrow \infty} 0$ .

The reverse inequality  $P_Y(T_\delta^n(Y|x^n)) \geq 2^{-n[I(X;Y)+\beta_n+\alpha_n]}$  can be proved following similar argument. ■

### B. Graphical Representation of Probability Distributions

Following [64, Section II], we use in this paper a technique based on undirected graphs, that provides a sufficient condition for establishing Markov chains from a joint distribution. Such a technique for establishing conditional independence was introduced in [65] for Bayesian networks, and further generalized to various types of graphs [66]. This paragraph recalls the main points of this technique.

Assume that a sequence of random variables  $X^n$  has joint distribution with the following form:

$$p(x^n) = f_1(x_{S_1})f_2(x_{S_2}) \cdots f_k(x_{S_k}) ,$$

where, for each  $i \in \{1, \dots, k\}$ ,  $S_i$  is a subset of  $\{1, \dots, n\}$ , notation  $x_{S_i}$  stands for collection  $(x_j)_{j \in S_i}$ , and  $f_i$  is some nonnegative function.

1) *Drawing the graph:* Draw an undirected graph where all involved random variables *e.g.*,  $(X_j)_{j \in \{1, \dots, n\}}$ , are nodes. For each  $i \in \{1, \dots, k\}$ , draw edges between all the nodes in  $X_{S_i}$ .

2) *Checking Markov relations:* Let  $\mathcal{G}_1$ ,  $\mathcal{G}_2$ , and  $\mathcal{G}_3$  be three disjoint subsets of  $\{1, \dots, n\}$ . If all paths in the graph from a node in  $X_{\mathcal{G}_1}$  to a node in  $X_{\mathcal{G}_3}$  pass through a node in  $X_{\mathcal{G}_2}$ , then  $X_{\mathcal{G}_1} \perp\!\!\!\perp X_{\mathcal{G}_3} \mid X_{\mathcal{G}_2}$  form a Markov chain. The proof of this result can be found in [64] and is omitted here.

### C. Csiszár and Körner's Equality

*Lemma 5 (Csiszár and Körner's equality [28, Lemma 7]):* Consider two i.i.d. sequences  $X^n$  and  $Y^n$ , and a constant  $C$ . The following identity holds true:

$$\sum_{i=1}^n I(Y_{i+1}^n; X_i | C X^{i-1}) = \sum_{j=1}^n I(X^{j-1}; Y_j | C Y_{j+1}^n) .$$

*Proof:* From the chain rule for conditional mutual information, we can write:

$$\begin{aligned}
\sum_{i=1}^n I(Y_{i+1}^n; X_i | CX^{i-1}) &= \sum_{i=1}^n \sum_{j=i+1}^n I(Y_j; X_i | CX^{i-1} Y_{j+1}^n) \\
&= \sum_{i,j: i < j} I(Y_j; X_i | CX^{i-1} Y_{j+1}^n) \\
&= \sum_{j=1}^n \sum_{i=1}^{j-1} I(X_i; Y_j | CX^{i-1} Y_{j+1}^n) \\
&= \sum_{j=1}^n I(X^{j-1}; Y_j | CY_{j+1}^n) .
\end{aligned}$$

■

## APPENDIX B

### PROOF OF THEOREM 1 (INNER BOUND)

Let  $U, V, W$  be three random variables on finite sets  $\mathcal{U}, \mathcal{V}, \mathcal{W}$ , respectively, such that  $p(uvwace) = p(u|v)p(v|a)p(w|c)p(ace)$ , a function  $\hat{A} : \mathcal{V} \times \mathcal{W} \rightarrow \mathcal{A}$ , and a tuple  $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ . In this section, we describe a scheme that achieves (under some sufficient conditions) tuple  $(R_A, R_C, D, \Delta)$  i.e., for any  $\varepsilon > 0$ , we construct an  $(n, R_A + \varepsilon, R_C + \varepsilon)$ -code  $(f_A, f_C, g)$  such that:

$$\begin{aligned}
\mathbb{E}[d(A^n, g(f_A(A^n), f_C(C^n)))] &\leq D + \varepsilon , \\
\frac{1}{n} H(A^n | f_A(A^n), E^n) &\geq \Delta - \varepsilon .
\end{aligned}$$

In this scheme, Alice (resp. Charlie) transmits to Bob a compressed version  $(U, V)$ , with  $V$  on the top of  $U$ , (resp.  $W$ ) of  $A$  (resp.  $C$ ) using random binning. From the three bin indices, Bob *jointly* decodes variables  $U, V$  and  $W$ .

Let  $\varepsilon > 0$ ,  $R_1, R_2 \in \mathbb{R}_+^*$  such that  $R_1 + R_2 = R_A + \varepsilon$ , and  $S_1 \geq R_1, S_2 \geq R_2, S_C \geq R_C + \varepsilon$ . Define  $\gamma = \frac{\varepsilon}{8d_{\max}}$ .

#### A. Codebook generation at Alice

Randomly pick  $2^{nS_1}$  sequences  $u^n(s_1)$  from  $T_\delta^n(U)$  and divide them into  $2^{nR_1}$  equal size bins  $\{B_1(r_1)\}_{r_1 \in \{1, \dots, 2^{nR_1}\}}$ . Then, for each codeword  $u^n(s_1)$ , randomly pick  $2^{nS_2}$  sequences  $v^n(s_1, s_2)$  from  $T_\delta^n(V|u^n(s_1))$  and divide them into  $2^{nR_2}$  equal size bins  $\{B_2(s_1, r_2)\}_{r_2 \in \{1, \dots, 2^{nR_2}\}}$ .

### B. Codebook generation at Charlie

Randomly pick  $2^{nS_C}$  sequences  $w^n(s)$  from  $T_\delta^n(W)$  and divide them into  $2^{n(R_C+\varepsilon)}$  equal size bins  $\{B_C(r)\}_{r \in \{1, \dots, 2^{n(R_C+\varepsilon)}\}}$ .

### C. Encoding at Alice

Assume that sequence  $A^n$  is produced at Alice. Look for the first codeword  $u^n(s_1)$  such that  $(u^n(s_1), A^n) \in T_\delta^n(U, A)$ . Then look for a codeword  $v^n(s_1, s_2)$  such that  $(v^n(s_1, s_2), A^n) \in T_\delta^n(V, A|u^n(s_1))$ . Let  $B_1(r_1)$  and  $B_2(s_1, r_2)$  be the bins of  $u^n(s_1)$  and  $v^n(s_1, s_2)$ , respectively. Alice sends the message  $J = f_A(A^n) \triangleq (r_1, r_2)$  on her error-free link.

### D. Encoding at Charlie

Assume that sequence  $C^n$  is produced at Charlie. Look for a codeword  $w^n(s)$  such that  $(w^n(s), C^n) \in T_\delta^n(W, C)$ . Let  $B_C(r)$  be the bin of  $w^n(s)$ . Charlie sends the message  $K = f_C(C^n) \triangleq r$  on his error-free link.

### E. Decoding at Bob

Assume that Bob receives  $J = (r_1, r_2)$  from Alice and  $K = r$  from Charlie. Look for the unique *jointly typical* codewords  $(u^n, v^n, w^n)$  with bin indices  $(r_1, r_2, r)$  i.e., look for the unique indices  $(s_1, s_2, s)$  such that  $(u^n(s_1), v^n(s_1, s_2), w^n(s)) \in (B_1(r_1) \times B_2(s_1, r_2) \times B_C(r)) \cap T_\delta^n(U, V, W)$ . Then compute the estimate  $g(J, K) \in \mathcal{A}^n$  using the component-wise relation  $g_i(J, K) \triangleq \hat{A}(v_i(s_1, s_2), w_i(s))$  for each  $i = \{1, \dots, n\}$ .

### F. Errors and constraints

Denoting by E the event ‘‘An error occurred during the encoding or decoding steps,’’ we expand its probability (averaged over the set of all possible codebooks) as follows:  $\Pr\{E\} \leq P_0 + P_{e,1} + P_{e,2} + P_{e,3} + P_d$ , where each term corresponds to a particular error event, as detailed below. We derive sufficient conditions on the parameters that make each of these probabilities small.

1) : From standard properties of typical sequences (see Appendix A-A), there exists a sequence  $\eta_n \xrightarrow{n \rightarrow \infty} 0$  such that  $P_0 \triangleq \Pr\{(A^n, C^n, E^n) \notin T_\delta^n(A, C, E)\} \leq \eta_n$ . Consequently,  $P_0 \leq \gamma$  for some sufficiently large  $n$ .

2) : In the first encoding step, Alice needs to find (at least) one codeword  $u^n(s_1)$  such that  $(u^n(s_1), A^n) \in T_\delta^n(U, A)$ . The corresponding error probability  $P_{e,1}$  writes:

$$\begin{aligned}
P_{e,1} &\triangleq \Pr \{ \nexists s_1 \text{ s.t. } (u^n(s_1), A^n) \in T_\delta^n(U, A) \} \\
&= \left( \Pr \left\{ (U^n, A^n) \notin T_\delta^n(U, A) \mid U^n \in T_\delta^n(U), A^n \in T_\delta^n(A) \right\} \right)^{2^{nS_1}} \\
&= \left( 1 - \Pr \left\{ (U^n, A^n) \in T_\delta^n(U, A) \mid U^n \in T_\delta^n(U), A^n \in T_\delta^n(A) \right\} \right)^{2^{nS_1}} \\
&\leq 2^{-2^{nS_1} \Pr \{ (U^n, A^n) \in T_\delta^n(U, A) \mid U^n \in T_\delta^n(U), A^n \in T_\delta^n(A) \}} \\
&\leq 2^{-2^{nS_1} 2^{-n(I(U;A) + \eta_n)}},
\end{aligned}$$

for some sequence  $\eta_n \xrightarrow[n \rightarrow \infty]{} 0$  (see Lemma 4 in Appendix A-A). If  $S_1 > I(U; A)$ , then probability  $P_{e,1}$  vanishes as  $n$  tends to infinity, and hence can be upper bounded by  $\gamma$  for some sufficiently large  $n$ .

Similarly, the second encoding step requires condition  $S_2 > I(V; A|U)$  to succeed with probability  $1 - P_{e,2} \geq 1 - \gamma$ .

3) : In his encoding step, Charlie needs to find (at least) one codeword  $w^n(s)$  such that  $(w^n(s), C^n) \in T_\delta^n(W, C)$ . Following the above argument, this requires condition  $S_C > I(W; C)$  to succeed with probability  $1 - P_{e,3} \geq 1 - \gamma$ .

4) : The decoding error probability  $P_d$  must be carefully handled. An error occurs when the decoded tuple differ from the original one  $(s_1, s_2, s)$ . There are three meaningful possible events so that  $P_d$  writes:<sup>3</sup>

$$\begin{aligned}
P_d &\triangleq \Pr \{ \overline{(s_1, s_2, s)} \} \\
&= \Pr \{ \{ \overline{s} \} \cup \{ \overline{s_1}, \check{s} \} \cup \{ \check{s}_1, \overline{s_2}, \check{s} \} \} \\
&\leq \Pr \{ \overline{s} \} + \Pr \{ \overline{s_1}, \check{s} \} + \Pr \{ \check{s}_1, \overline{s_2}, \check{s} \} .
\end{aligned}$$

We now study each term of the r.h.s. of the above equation.

<sup>3</sup>We denote by  $\check{s}$  the event “Index  $s$  has been correctly decoded”, and  $\overline{s}$  its complement. Same notation holds for indices  $s_1$ ,  $s_2$ , and any tuple of indices.

$$\begin{aligned}
\Pr \{\mathcal{S}\} &= \Pr \left\{ \exists s'_1, s'_2, s' \neq s \text{ s.t.} \right. \\
&\quad \left. (u^n(s'_1), v^n(s'_1, s'_2), w^n(s')) \in (B_1(r_1) \times B_2(s'_1, r_2) \times B_C(r)) \cap T_\delta^n(U, V, W) \right\} \\
&\leq 2^{n(S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon)} \\
&\quad \times \Pr \left\{ (U^n, V^n, W^n) \in T_\delta^n(U, V, W) \mid (U^n, V^n) \in T_\delta^n(U, V), W^n \in T_\delta^n(W) \right\} \\
&\leq 2^{n(S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon)} 2^{-n(I(UV;W) - \eta_n)} \\
&= 2^{n(S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon - I(V;W) + \eta_n)},
\end{aligned}$$

for some sequence  $\eta_n \xrightarrow{n \rightarrow \infty} 0$  (see Lemma 4 in Appendix A-A). If  $S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon < I(V;W)$ , then the above probability vanishes as  $n$  tends to infinity, and hence can be upper bounded by  $\gamma$  for some sufficiently large  $n$ .

$$\begin{aligned}
\Pr \{\mathcal{S}_1, \check{s}\} &= \Pr \left\{ \exists s'_1 \neq s_1, s'_2 \text{ s.t.} \right. \\
&\quad \left. (u^n(s'_1), v^n(s'_1, s'_2), w^n(s)) \in (B_1(r_1) \times B_2(s'_1, r_2) \times B_C(r)) \cap T_\delta^n(U, V, W) \right\} \\
&\leq 2^{n(S_1 - R_1 + S_2 - R_2)} \\
&\quad \times \Pr \left\{ (U^n, V^n, W^n) \in T_\delta^n(U, V, W) \mid (U^n, V^n) \in T_\delta^n(U, V), W^n \in T_\delta^n(W) \right\},
\end{aligned}$$

Following the above argument, if  $S_1 - R_1 + S_2 - R_2 < I(V;W)$ , then the above probability can be upper bounded by  $\gamma$  for some sufficiently large  $n$ .

$$\begin{aligned}
\Pr \{\check{s}_1, \mathcal{S}_2, \check{s}\} &= \Pr \left\{ \exists s'_2 \neq s_2 \text{ s.t.} \right. \\
&\quad \left. (u^n(s_1), v^n(s_1, s'_2), w^n(s)) \in (B_1(r_1) \times B_2(s_1, r_2) \times B_C(r)) \cap T_\delta^n(U, V, W) \right\} \\
&\leq 2^{n(S_2 - R_2)} \\
&\quad \times \Pr \left\{ (U^n, V^n, W^n) \in T_\delta^n(U, V, W) \mid (U^n, V^n) \in T_\delta^n(U, V), (U^n, W^n) \in T_\delta^n(U, W) \right\} \\
&\leq 2^{n(S_2 - R_2)} 2^{-n(I(V;W|U) - \eta_n)},
\end{aligned}$$

for some sequence  $\eta_n \xrightarrow{n \rightarrow \infty} 0$ . If  $S_2 - R_2 < I(V;W|U)$ , then the above probability vanishes as  $n$  tends to infinity, and hence  $\Pr\{\check{s}_1, \mathcal{S}_2, \check{s}\} \leq \gamma$ , for some sufficiently large  $n$ .

5) *Summary:* In this paragraph, we proved that under some sufficient conditions,  $\Pr \{E\} \leq 7\gamma$ .

### G. Distortion at Bob

We now check that our code achieves the required distortion level at Bob (averaged over the set of all possible codebooks):

$$\begin{aligned} \mathbb{E} \left[ d(A^n, g(f_A(A^n), f_C(C^n))) \right] &\leq (1 - \Pr \{E\}) \mathbb{E} \left[ d(A^n, \hat{A}(v^n(s_1, s_2), w^n(s))) \middle| \bar{E} \right] + \Pr \{E\} d_{\max} \\ &\leq \mathbb{E} [d(A, \hat{A}(V, W))] + \frac{\varepsilon}{8} + \frac{7\varepsilon}{8}, \end{aligned}$$

where the last inequality holds for some sufficiently large  $n$ , and follows from  $\Pr \{E\} \leq 7\gamma$ , the definition of  $\gamma$ , and the argument below: For each  $(a^n, v^n, w^n) \in T_\delta^n(A, V, W)$ ,

$$\begin{aligned} d(a^n, \hat{A}(v^n, w^n)) &= \frac{1}{n} \sum_{i=1}^n d(a_i, \hat{A}(v_i, w_i)) \\ &= \frac{1}{n} \sum_{(a,v,w) \in \mathcal{A} \times \mathcal{V} \times \mathcal{W}} d(a, \hat{A}(v, w)) N(a, v, w | a^n, v^n, w^n) \\ &= \mathbb{E} [d(A, \hat{A}(V, W))] \\ &\quad + \sum_{(a,v,w) \in \mathcal{A} \times \mathcal{V} \times \mathcal{W}} d(a, \hat{A}(v, w)) \left( \frac{1}{n} N(a, v, w | a^n, v^n, w^n) - p(a, v, w) \right) \\ &\leq \mathbb{E} [d(A, \hat{A}(V, W))] + d_{\max} \|\mathcal{A}\| \|\mathcal{V}\| \|\mathcal{W}\| \delta_n, \end{aligned}$$

where the last inequality holds since  $(a^n, v^n, w^n) \in T_\delta^n(A, V, W)$ . The result follows from the fact that  $(A^n, v^n(s_1, s_2), w^n(s)) \in T_\delta^n(A, V, W)$  when no error occurred, and  $\delta_n \xrightarrow{n \rightarrow \infty} 0$  (see the Delta-Convention in Appendix A-A). For some sufficiently large  $n$ ,  $d_{\max} \|\mathcal{A}\| \|\mathcal{V}\| \|\mathcal{W}\| \delta_n \leq \frac{\varepsilon}{8}$ .

Condition  $D \geq \mathbb{E} [d(A, \hat{A}(V, W))]$  is thus sufficient to achieve distortion  $D + \varepsilon$  at Bob.

### H. Equivocation rate at Eve

The equivocation rate at Eve (averaged over the set of all possible codebooks) can be lower bounded as follows:

$$\begin{aligned} \frac{1}{n} H(A^n | f_A(A^n), E^n) &= \frac{1}{n} H(A^n | r_1 r_2 E^n) \\ &= \frac{1}{n} \left[ H(A^n | r_1 E^n) - I(A^n; r_2 | r_1 E^n) \right] \\ &\stackrel{(a)}{\geq} \frac{1}{n} \left[ H(A^n | s_1 E^n) - H(r_2) \right] \\ &\stackrel{(b)}{\geq} H(A | UE) - R_2 - \varepsilon, \end{aligned}$$



where

- step (a) follows from the facts that the bin index  $r_1$  is a deterministic function of the codeword index  $s_1$ , the bin index  $r_2$  is a deterministic function of  $A^n$ , and conditioning reduces the entropy,
- step (b) for some sufficiently large  $n$ , from the fact that the codewords  $u^n(s_1)$  are drawn i.i.d. (see Lemma 6 below), and  $r_2 \in \{1, \dots, 2^{nR_2}\}$ .

Condition  $\Delta \leq H(A|UE) - R_2$  is thus sufficient to achieve equivocation rate  $\Delta - \varepsilon$  at Eve.

*Lemma 6:* The following inequality holds for some sequence  $\eta_n \xrightarrow[n \rightarrow \infty]{} 0$ :

$$H(A^n|s_1 E^n) \geq n(H(A|UE) - \eta_n) .$$

*Proof:* Since the codeword index  $s_1$  is a deterministic function of  $A^n$ , term  $H(A^n|s_1 E^n)$  writes

$$\begin{aligned} H(A^n|s_1 E^n) &= H(A^n E^n|s_1) - H(E^n|s_1) \\ &= H(A^n E^n) - H(s_1) - H(E^n|s_1) . \end{aligned} \quad (28)$$

We now study each term of the r.h.s. of the above equation.

Variables  $A_i, E_i$  are i.i.d., hence  $H(A^n E^n) = nH(AE)$ .

The second term is studied through the distribution of index  $s_1$ , using classical argument of typical sequences and random coding. From the encoding procedure described in Section B-C, the distribution of  $s_1$  writes, for each  $j \in \{1, \dots, 2^{nS_1}\}$ :

$$\begin{aligned} \Pr \{s_1 = j\} &= \Pr \left\{ (u^n(j), A^n) \in T_\delta^n(U, A) \cap \bigcap_{i=1}^{j-1} ((u^n(i), A^n) \notin T_\delta^n(U, A)) \right\} \\ &= t_n(1 - t_n)^{j-1} , \end{aligned}$$

where  $t_n \triangleq \Pr \left\{ (U^n, A^n) \in T_\delta^n(U, A) \mid U^n \in T_\delta^n(U), A^n \in T_\delta^n(A) \right\}$ . The entropy of index  $s_1$  thus writes

$$H(s_1) = - \sum_{j=1}^{2^{nS_1}} t_n(1 - t_n)^{j-1} \log(t_n(1 - t_n)^{j-1}) - P_{e,1} \log(P_{e,1}) ,$$

where  $P_{e,1}$  is the error probability of this encoding step. From Section B-F, if  $S_1 > I(U; A)$ , then probability  $P_{e,1}$  vanishes as  $n$  tends to infinity. Since each term  $t_n(1 - t_n)^{j-1}$  is non-negative

and  $x \log x \xrightarrow{x \rightarrow 0^+} 0^-$ , the above entropy can be upper bounded as follows:

$$H(s_1) \leq - \sum_{j=1}^{\infty} t_n (1 - t_n)^{j-1} \log(t_n (1 - t_n)^{j-1}) + \eta_n^{(1)} , \quad (29)$$

for some sequence  $\eta_n^{(1)} \xrightarrow{n \rightarrow \infty} 0$ . The above series writes

$$\begin{aligned} \sum_{j=1}^{\infty} t_n (1 - t_n)^{j-1} \log(t_n (1 - t_n)^{j-1}) \\ = t_n \log(t_n) \sum_{j=1}^{\infty} (1 - t_n)^{j-1} + t_n \log(1 - t_n) \sum_{j=1}^{\infty} (j-1) (1 - t_n)^{j-1} . \end{aligned}$$

Equation (29) thus yields the following upper bound:

$$H(s_1) \leq -\log(t_n) - \log(1 - t_n) \frac{1 - t_n}{t_n} + \eta_n^{(1)} .$$

Now, from standard results on typical sequences (see Appendix A-A),  $2^{-n(I(U;A) + \eta_n^{(2)})} \leq t_n \leq 2^{-n(I(U;A) - \eta_n^{(2)})}$  for some sequence  $\eta_n^{(2)} \xrightarrow{n \rightarrow \infty} 0$ . Since  $\frac{\log(1-x)}{x} \xrightarrow{x \rightarrow 0} -1$ , this yields

$$H(s_1) \leq n(I(U; A) + \eta_n^{(2)}) + 1 + \eta_n^{(3)} + \eta_n^{(1)} ,$$

for some sequence  $\eta_n^{(3)} \xrightarrow{n \rightarrow \infty} 0$ .

The third term can be studied following the argument of [34, Section 2.3] for the wiretap channel. The equivalent of Equation (2.54) of [34] here writes

$$H(E^n | s_1) \leq n (H(E|U) + \eta_n^{(4)}) ,$$

for some sequence  $\eta_n^{(4)} \xrightarrow{n \rightarrow \infty} 0$ .

Equation (28) along with the above results yields

$$\frac{1}{n} H(A^n | s_1 E^n) \geq H(AE) - I(U; A) - \eta_n^{(2)} - \frac{1 + \eta_n^{(3)} + \eta_n^{(1)}}{n} - H(E|U) - \eta_n^{(4)} . \quad (30)$$

Using the Markov chain  $U \dashv\vdash A \dashv\vdash E$ , this proves Lemma 6. ■

### I. End of Proof

In this section, we proved that sufficient conditions for the achievability of a tuple  $(R_A, R_C, D, \Delta)$  are given by the following system of inequalities, for each  $\varepsilon > 0$ :

$$\left\{ \begin{array}{l} R_1 > 0 \\ R_2 > 0 \\ R_A + \varepsilon = R_1 + R_2 \\ R_C \geq 0 \\ S_1 \geq R_1 \\ S_2 \geq R_2 \\ S_C \geq R_C + \varepsilon \\ S_1 > I(U; A) \\ S_2 > I(V; A|U) \\ S_C > I(W; C) \\ S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon < I(V; W) \\ S_1 - R_1 + S_2 - R_2 < I(V, W) \\ S_2 - R_2 < I(V; W|U) \\ D \geq \mathbb{E}[d(A, \hat{A}(V, W))] \\ \Delta \leq H(A|UE) - R_2 \end{array} \right.$$

Fourier-Motzkin elimination then yields:

$$\left\{ \begin{array}{l} R_A + \varepsilon > I(V; A|W) \\ R_C + \varepsilon > I(W; C|V) \\ R_A + R_C + 2\varepsilon > I(VW; AC) \\ D \geq \mathbb{E}[d(A, \hat{A}(V, W))] \\ \Delta < H(A|VW) + I(A; W|U) - I(A; E|U) \\ \Delta - R_C - \varepsilon < H(A|V) - I(A; E|U) - I(W; C|V) \end{array} \right.$$

This proves Theorem 1. ■

## APPENDIX C

## PROOF OF PROPOSITION 1 (BOUNDS ON THE CARDINALITIES)

A. *Bound on  $\|\mathcal{W}\|$* 

First, note that the single-letter inequalities of Theorem 1 can be written as follows:

$$\begin{aligned}
R_A &\geq I(V; A|W) , \\
R_C &\geq H(C|V) - H(C|VW) , \\
R_A + R_C &\geq I(V; A) + H(C|V) - H(C|VW) , \\
D &\geq \mathbb{E}[d(A, \hat{A}(V, W))] , \\
\Delta &\leq H(A|UE) - I(V; A|W) + I(U; A|W) , \\
\Delta - R_C &\leq H(A|V) - I(A; E|U) - H(C|V) + H(C|VW) .
\end{aligned}$$

We then use Fenchel-Eggleston-Carathéodory's theorem and follow standard arguments (see [52, Appendix C]). Consider the following  $\|\mathcal{C}\| + 3$  continuous functions of  $p(c|w)$ :

$$\begin{aligned}
&p(c|w) , \\
&I(V; A|W = w) , \\
&H(C|V, W = w) = H(CV|W = w) - H(V|W = w) , \\
&\mathbb{E}[d(A, \hat{A}(V, W))|W = w] , \\
&I(U; A|W = w)
\end{aligned}$$

From Fenchel-Eggleston-Carathéodory's theorem, there exists a random variable  $W'$  on  $\mathcal{W}'$  with  $\|\mathcal{W}'\| \leq \|\mathcal{C}\| + 3$  such that  $p(c)$ ,  $I(V; A|W)$ ,  $H(C|VW)$ ,  $\mathbb{E}[d(A, \hat{A}(V, W))]$  and  $I(U; A|W)$  are preserved.

### B. Bounds on $\|\mathcal{U}\|$ and $\|\mathcal{V}\|$

We now rewrite the inequalities of Theorem 1 as follows:

$$\begin{aligned}
R_A &\geq H(A|W) - H(A|VW) , \\
R_C &\geq I(W; C|V) , \\
R_A + R_C &\geq I(W; C) + H(A|W) - H(A|VW) , \\
D &\geq \mathbb{E}[d(A, \hat{A}(V, W))] , \\
\Delta &\leq H(A|VW) + I(A; W|U) - I(A; E|U) , \\
\Delta - R_C &\leq H(A|V) - I(A; E|U) - I(W; C|V) .
\end{aligned}$$

Consider the following  $\|\mathcal{A}\| + 5$  continuous functions of  $p(v|u)$ :

$$\begin{aligned}
p(a|u) &= \mathbb{E}[p(a|V)|U = u] , \\
H(A|VW, U = u) &= H(AVW|U = u) - H(VW|U = u) , \\
I(W; C|V, U = u) &= I(W; C|U = u) - I(W; V|U = u) , \\
\mathbb{E}[d(A, \hat{A}(V, W))|U = u] &, \\
I(A; W|U = u) &, \\
I(A; E|U = u) &, \\
H(A|V, U = u) &= H(AV|U = u) - H(V|U = u) .
\end{aligned}$$

From Fenchel-Eggleston-Carathéodory's theorem, there exists a random variable  $U'$  on  $\mathcal{U}'$  with  $\|\mathcal{U}'\| \leq \|\mathcal{A}\| + 5$  such that  $p(a)$ ,  $H(A|VW)$ ,  $I(W; C|V)$ ,  $\mathbb{E}[d(A, \hat{A}(V, W))]$ ,  $I(A; W|U)$ ,  $I(A; E|U)$ , and  $H(A|V)$  are preserved.

Now, for each  $u' \in \mathcal{U}'$ , consider the following  $\|\mathcal{A}\| + 3$  continuous functions of  $p(a|u', v)$ :

$$\begin{aligned}
p(a|u', v) &, \\
H(A|W, U' = u', V = v) &= H(AW|U' = u', V = v) - H(W|U' = u', V = v) , \\
I(W; C|U' = u', V = v) &, \\
\mathbb{E}[d(A, \hat{A}(V, W))|U' = u', V = v] &, \\
H(A|U' = u', V = v) &.
\end{aligned}$$

From Fenchel-Eggleston-Carathéodory's theorem, there exists a set  $\mathcal{V}'$  with  $\|\mathcal{V}'\| \leq \|\mathcal{A}\| + 3$  and, for each  $u' \in \mathcal{U}'$ , a random variable  $V'|\{U' = u'\}$  on  $\mathcal{V}'$  and a function  $\hat{A}'_{u'} : \mathcal{V}' \times \mathcal{W} \rightarrow \mathcal{A}$ , such that  $p(a|u')$ ,  $H(A|VW, U' = u')$ ,  $I(W; C|V, U' = u')$ ,  $\mathbb{E}[d(A, \hat{A}(V, W))|U' = u']$ , and  $H(A|V, U' = u')$  are preserved.

Then define set  $\mathcal{V}'' = \mathcal{U}' \times \mathcal{V}'$ , random variable  $V'' = (U', V')$  and function  $\hat{A}'' : \mathcal{V}'' \times \mathcal{W} \rightarrow \mathcal{A}$  by  $\hat{A}''(v'', w) = \hat{A}''(u', v', w) \triangleq \hat{A}'_{u'}(v', w)$ . From the above cardinality bounds,  $\|\mathcal{V}''\| \leq (\|\mathcal{A}\| + 5)(\|\mathcal{A}\| + 3)$ . Note that  $U' \ominus V'' \ominus A \ominus (C, E)$  form a Markov chain. From these new definitions and previous constructions, we check that quantities involving variable  $V$  are preserved:

$$\begin{aligned} H(A|V''W) &= H(A|U'V'W) \\ &= H(A|U'VW) \\ &= H(A|VW) , \end{aligned}$$

$$\begin{aligned} I(W; C|V'') &= I(W; C|U'V') \\ &= I(W; C|U'V) \\ &= I(W; C|V) , \end{aligned}$$

$$\begin{aligned} \mathbb{E}[d(A, \hat{A}''(V'', W))] &= \mathbb{E}[d(A, \hat{A}'_{U'}(V', W))] \\ &= \mathbb{E}\left[\mathbb{E}[d(A, \hat{A}'_{U'}(V', W))|U']\right] \\ &= \mathbb{E}\left[\mathbb{E}[d(A, \hat{A}(V, W))|U']\right] \\ &= \mathbb{E}[d(A, \hat{A}(V, W))] , \end{aligned}$$

and

$$\begin{aligned} H(A|V'') &= H(A|U'V') \\ &= H(A|U'V) \\ &= H(A|V) . \end{aligned}$$

This proves Proposition 1. ■

## APPENDIX D

## PROOF OF THEOREM 2 (OUTER BOUND)

In this section, we prove Theorem 2. Let  $(R_A, R_C, D, \Delta)$  be an achievable tuple and  $\varepsilon > 0$ . There exists an  $(n, R_A + \varepsilon, R_C + \varepsilon)$ -code  $(f_A, f_C, g)$  s.t.:

$$\begin{aligned} \mathbb{E}[d(A^n, g(f_A(A^n), f_C(C^n)))] &\leq D + \varepsilon, \\ \frac{1}{n} H(A^n | f_A(A^n), E^n) &\geq \Delta - \varepsilon. \end{aligned}$$

Denote by  $J = f_A(A^n)$  and  $K = f_C(C^n)$  the messages transmitted by Alice and Charlie, respectively. From these definitions and the fact that random variables  $A_i, C_i, E_i$  are independent across time, the joint distribution of  $(J, K, A^n, C^n, E^n)$  can be written as follows:

$$p(j, k, a^n, c^n, e^n) = \mathbb{I}_{f_A(a^n)}(j) \mathbb{I}_{f_C(c^n)}(k) p(a^{i-1}, c^{i-1}, e^{i-1}) p(a_i, c_i, e_i) p(a_{i+1}^n, c_{i+1}^n, e_{i+1}^n).$$

Following the technique described in Appendix A-B and using the above expansion, we can obtain the graphs of Fig. 16.

For each  $i \in \{1, \dots, n\}$ , define random variables  $U_i, V_i$  and  $W_i$  as follows:

$$U_i = (J, A^{i-1}, E^{i-1}), \quad (31)$$

$$V_i = (J, A^{i-1}, C^{i-1}, E^{i-1}), \quad (32)$$

$$W_i = (K, C^{i-1}). \quad (33)$$

From Fig. 16,  $U_i \text{---} V_i \text{---} A_i \text{---} (C_i, E_i)$  and  $W_i \text{---} C_i \text{---} (A_i, E_i)$  form Markov chains (see Appendix A-B for details on this graphical technique for checking Markov relations).

Following the usual technique, we also define an independent random variable  $Q$  uniformly distributed over the set  $\{1, \dots, n\}$ , and  $A = A_Q, C = C_Q, E = E_Q, U = (Q, U_Q), V = (Q, V_Q)$ , and  $W = (Q, W_Q)$ . Note that  $U \text{---} V \text{---} A \text{---} (C, E)$  and  $W \text{---} C \text{---} (A, E)$  still form Markov chains, and that  $(A, C, E)$  is distributed according to the joint distribution  $p(a, c, e)$  i.e., the original distribution of  $(A_i, C_i, E_i)$ .

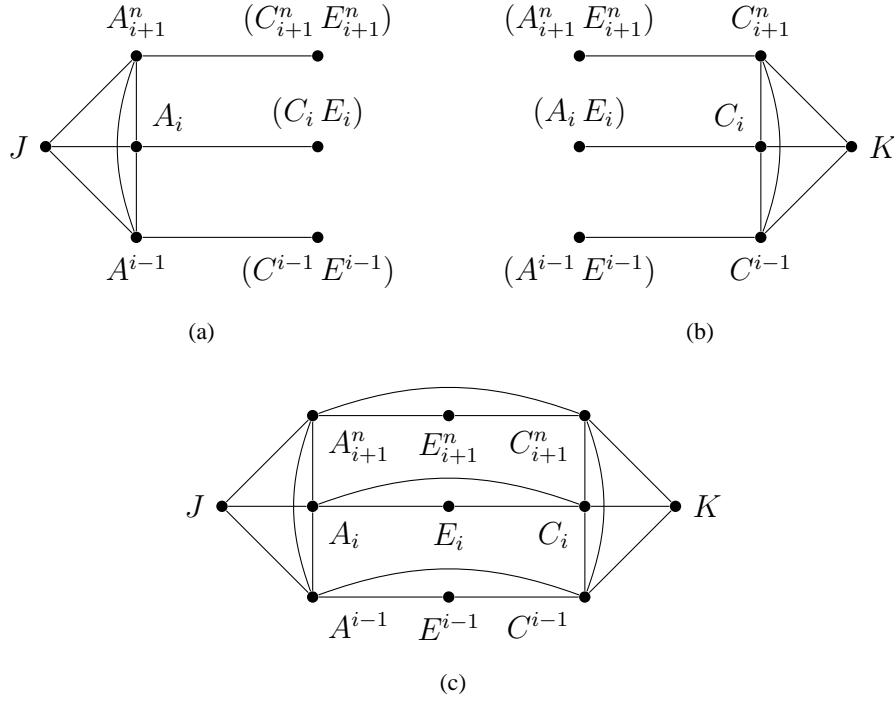


Figure 16: Outer bound—Graphical representation of probability distributions (a)  $p(j, a^n, c^n, e^n)$ , (b)  $p(k, a^n, c^n, e^n)$  and (c)  $p(j, k, a^n, c^n, e^n)$ .

#### A. Rate at Alice

$$\begin{aligned}
 n(R_A + \varepsilon) &\geq H(J) \\
 &\stackrel{(a)}{=} I(J; K A^n C^n E^n) \\
 &\stackrel{(b)}{\geq} I(J; A^n C^n E^n | K) \\
 &\stackrel{(c)}{=} \sum_{i=1}^n I(J; A_i C_i E_i | K A^{i-1} C^{i-1} E^{i-1}) \\
 &= \sum_{i=1}^n \left[ I(J A^{i-1} E^{i-1}; A_i C_i E_i | K C^{i-1}) - I(A^{i-1} E^{i-1}; A_i C_i E_i | K C^{i-1}) \right] \\
 &\stackrel{(d)}{=} \sum_{i=1}^n I(J A^{i-1} C^{i-1} E^{i-1}; A_i C_i E_i | K C^{i-1}) \\
 &\stackrel{(e)}{\geq} \sum_{i=1}^n I(V_i; A_i | W_i) ,
 \end{aligned}$$



where

- step (a) follows from  $J = f_A(A^n)$ ,
- step (b) from the non-negativity of mutual information,
- step (c) from the chain rule for conditional mutual information,
- step (d) from the Markov chain  $(A_i, C_i, E_i) \text{---} (K, C^{i-1}) \text{---} (A^{i-1}, E^{i-1})$  (see Fig. 16b),
- step (e) from the non-negativity of mutual information and definitions (32), (33).

Using random variable  $Q$ , this yields

$$\begin{aligned} R_A + \varepsilon &\geq \frac{1}{n} \sum_{i=1}^n I(V_Q; A_Q | W_Q, Q = i) \\ &= I(V_Q; A_Q | W_Q Q) \\ &= I(V; A | W) . \end{aligned}$$

### B. Rate at Charlie

Using similar arguments with  $K = f_C(C^n)$ , we can obtain:

$$\begin{aligned} n(R_C + \varepsilon) &\geq H(K) \\ &\stackrel{(a)}{=} I(K; J A^n C^n E^n) \\ &\stackrel{(b)}{\geq} I(K; A^n C^n E^n | J) \\ &\stackrel{(c)}{=} \sum_{i=1}^n I(K; A_i C_i E_i | J A^{i-1} C^{i-1} E^{i-1}) \\ &= \sum_{i=1}^n I(K C^{i-1}; A_i C_i E_i | J A^{i-1} C^{i-1} E^{i-1}) \\ &\stackrel{(d)}{\geq} \sum_{i=1}^n I(W_i; C_i | V_i) , \end{aligned}$$

where

- step (a) follows from  $K = f_C(C^n)$ ,
- step (b) from the non-negativity of mutual information,
- step (c) from the chain rule for conditional mutual information,
- step (d) from the non-negativity of mutual information and definitions (32), (33).

Then, using auxiliary random variable  $Q$ ,

$$\begin{aligned} R_C + \varepsilon &\geq \frac{1}{n} \sum_{i=1}^n I(W_Q; C_Q | V_Q, Q = i) \\ &= I(W; C | V) . \end{aligned}$$

### C. Sum-rate

$$\begin{aligned} n(R_A + R_C + 2\varepsilon) &\geq H(JK) \\ &\stackrel{(a)}{=} I(JK; A^n C^n E^n) \\ &\stackrel{(b)}{=} \sum_{i=1}^n I(JK; A_i C_i E_i | A^{i-1} C^{i-1} E^{i-1}) \\ &= \sum_{i=1}^n \left[ I(JK A^{i-1} C^{i-1} E^{i-1}; A_i C_i E_i) - I(A^{i-1} C^{i-1} E^{i-1}; A_i C_i E_i) \right] \\ &\stackrel{(c)}{=} \sum_{i=1}^n I(JK A^{i-1} C^{i-1} E^{i-1}; A_i C_i E_i) \\ &\stackrel{(d)}{\geq} \sum_{i=1}^n I(V_i W_i; A_i C_i) , \end{aligned}$$

where

- step (a) follows from  $J = f_A(A^n)$  and  $K = f_C(C^n)$ ,
- step (b) from the chain rule for mutual information,
- step (c) from the fact that random variables  $A_i$ ,  $C_i$  and  $E_i$  are independent across time,
- step (d) from the non-negativity of mutual information and definitions (32), (33).

Using random variable  $Q$ , this yields

$$\begin{aligned} R_A + R_C + 2\varepsilon &\geq \frac{1}{n} \sum_{i=1}^n I(V_Q W_Q; A_Q C_Q | Q = i) \\ &= I(VW; AC) . \end{aligned}$$

### D. Distortion at Bob

Bob reconstructs  $g(J, K)$ . For each  $i \in \{1, \dots, n\}$ , define function  $\hat{A}_i$  as the  $i$ -th coordinate of this estimate:

$$\hat{A}_i(V_i, W_i) \triangleq g_i(J, K) .$$

The component-wise mean distortion at Bob thus verifies

$$\begin{aligned}
D + \varepsilon &\geq \mathbb{E}[d(A^n, g(J, K))] \\
&= \frac{1}{n} \sum_{i=1}^n \mathbb{E}[d(A_i, \hat{A}_i(V_i, W_i))] \\
&= \frac{1}{n} \sum_{i=1}^n \mathbb{E}[d(A_Q, \hat{A}_Q(V_Q, W_Q)) \mid Q = i] \\
&= \mathbb{E}[d(A_Q, \hat{A}_Q(V_Q, W_Q))] \\
&= \mathbb{E}[d(A, \hat{A}(V, W))] ,
\end{aligned}$$

where we defined function  $\hat{A}$  by

$$\hat{A}(V, W) = \hat{A}(Q, V_Q, W_Q) \triangleq \hat{A}_Q(V_Q, W_Q) .$$

### E. Equivocation rate at Eve

$$\begin{aligned}
n(\Delta - \varepsilon) &\leq H(A^n | JE^n) \\
&= H(A^n | J) - I(A^n; E^n | J) \\
&\stackrel{(a)}{=} H(A^n | J) - I(A^n; E^n) + I(J; E^n) \\
&\stackrel{(b)}{=} \sum_{i=1}^n \left[ H(A_i | JA^{i-1}) - I(A_i; E_i) + I(JE^{i-1}; E_i) \right] \\
&= \sum_{i=1}^n \left[ H(A_i | JKA^{i-1}C^{i-1}E^{i-1}) + I(A_i; KC^{i-1}E^{i-1} | JA^{i-1}) - I(A_i; E_i) + I(JE^{i-1}; E_i) \right] \\
&\stackrel{(c)}{\leq} \sum_{i=1}^n \left[ H(A_i | JKA^{i-1}C^{i-1}E^{i-1}) + I(A_i; KC^{i-1} | JA^{i-1}E^{i-1}) \right. \\
&\quad \left. + I(A_i; E^{i-1} | JA^{i-1}) - I(A_i; E_i) + I(JA^{i-1}E^{i-1}; E_i) \right] \\
&\stackrel{(d)}{=} \sum_{i=1}^n \left[ H(A_i | JKA^{i-1}C^{i-1}E^{i-1}) + I(A_i; KC^{i-1} | JA^{i-1}E^{i-1}) - I(A_i; E_i | JA^{i-1}E^{i-1}) \right] \\
&\stackrel{(e)}{=} \sum_{i=1}^n \left[ H(A_i | V_i W_i) + I(A_i; W_i | U_i) - I(A_i; E_i | U_i) \right] ,
\end{aligned}$$

where

- step (a) follows from the Markov chain  $J \multimap A^n \multimap E^n$  (see Fig. 16a),

- step (b) from the chain rules for conditional entropy and mutual information, and the fact that random variables  $A_i$  and  $E_i$  are independent across time,
- step (c) from standard identities and the non-negativity of conditional mutual information,
- step (d) from the Markov chain  $E_i \text{---} A_i \text{---} (JA^{i-1}) \text{---} E^{i-1}$  (see Fig. 16a),
- step (e) from definitions (31), (32) and (33).

Now, using auxiliary random variable  $Q$ ,

$$\begin{aligned}
 \Delta - \varepsilon &\leq \frac{1}{n} \sum_{i=1}^n \left[ H(A_Q | V_Q W_Q, Q = i) \right. \\
 &\quad \left. + I(A_Q; W_Q | U_Q, Q = i) - I(A_Q; E_Q | U_Q, Q = i) \right] \\
 &= H(A | VW) + I(A; W | U) - I(A; E | U) .
 \end{aligned}$$

#### F. Public-link secrecy rate

$$\begin{aligned}
 n(\Delta - R_C - 2\varepsilon) &\leq H(A^n | JE^n) - H(K) \\
 &\stackrel{(a)}{\leq} H(A^n | JE^n) - H(K | J) \\
 &\stackrel{(b)}{=} H(A^n | JE^n) - I(K; A^n C^n | J) \\
 &\stackrel{(c)}{=} \sum_{i=1}^n \left[ H(A_i | JA^{i-1} E^n) - I(K; A_i C_i | JA^{i-1} C^{i-1}) \right] \\
 &\stackrel{(d)}{\leq} \sum_{i=1}^n \left[ H(A_i | JA^{i-1} E^i) - I(K; C_i | JA^{i-1} C^{i-1}) \right] \\
 &\stackrel{(e)}{=} \sum_{i=1}^n \left[ H(A_i | JA^{i-1} C^{i-1} E^{i-1}) - I(A_i; E_i | JA^{i-1} E^{i-1}) \right. \\
 &\quad \left. - I(K C^{i-1}; C_i | JA^{i-1} C^{i-1} E^{i-1}) \right] \\
 &\stackrel{(f)}{=} \sum_{i=1}^n \left[ H(A_i | V_i) - I(A_i; E_i | U_i) - I(W_i; C_i | V_i) \right] ,
 \end{aligned}$$

where

- step (a) follows from the fact that conditioning reduces the entropy,
- step (b) from  $K = f_C(C^n)$ ,
- step (c) from the chain rules for conditional entropy and conditional mutual information,
- step (d) from the non-negativity of conditional mutual information,

- step (e) from the Markov chains  $A_i \text{---} (J, A^{i-1}) \text{---} (C^{i-1}, E^{i-1})$  (see Fig. 16a) and  $(K, C_i) \text{---} (J, A^{i-1}, C^{i-1}) \text{---} E^{i-1}$  (see Fig. 16c),
- step (f) from definitions (31), (32) and (33).

Using auxiliary random variable  $Q$ ,

$$\begin{aligned} \Delta - R_C - 2\varepsilon &\leq \frac{1}{n} \sum_{i=1}^n \left[ H(A_Q|V_Q, Q=i) - I(A_Q; E_Q|U_Q, Q=i) - I(W_Q; C_Q|V_Q, Q=i) \right] \\ &= H(A|V) - I(A; E|U) - I(W; C|V) . \end{aligned}$$

### G. End of Proof

We proved that, for each achievable tuple  $(R_A, R_C, D, \Delta)$  and each  $\varepsilon > 0$ , there exist random variables  $U, V$  and  $W$  such that  $U \text{---} V \text{---} A \text{---} (C, E)$  and  $W \text{---} C \text{---} (A, E)$  form Markov chains, and a function  $\hat{A}$  such that

$$\begin{aligned} R_A + \varepsilon &\geq I(V; A|W) , \\ R_C + \varepsilon &\geq I(W; C|V) , \\ R_A + R_C + 2\varepsilon &\geq I(VW; AC) , \\ D + \varepsilon &\geq \mathbb{E}[d(A, \hat{A}(V, W))] , \\ \Delta - \varepsilon &\leq H(A|VW) + I(A; W|U) - I(A; E|U) , \\ \Delta - R_C - 2\varepsilon &\leq H(A|V) - I(A; E|U) - I(W; C|V) , \end{aligned}$$

i.e.,  $(R_A + \varepsilon, R_C + \varepsilon, D + \varepsilon, \Delta - \varepsilon) \in \mathcal{R}_{\text{out}}$ . Recalling that region  $\mathcal{R}_{\text{out}}$  is closed, and letting  $\varepsilon$  tend to zero prove Theorem 2. ■

## APPENDIX E

### PROOF OF THE CONVERSE PART OF THEOREM 3

Let  $(R_A, D, \Delta)$  be an achievable tuple and  $\varepsilon > 0$ . There exists an  $(n, R_A + \varepsilon)$ -code  $(f, g)$  s.t.:

$$\begin{aligned} \mathbb{E}[d(A^n, g(f(A^n), C^n))] &\leq D + \varepsilon , \\ \frac{1}{n} H(A^n|f(A^n), E^n) &\geq \Delta - \varepsilon . \end{aligned}$$

Denote by  $J = f(A^n)$  the transmitted message, and define variables  $U_i$  and  $V_i$  as follows, for each  $i \in \{1, \dots, n\}$ :

$$U_i = (J, C_{i+1}^n, E^{i-1}) , \quad (34)$$

$$V_i = (J, A^{i-1}, C^{i-1}, C_{i+1}^n, E^{i-1}) . \quad (35)$$

From Fig. 16a,  $U_i \ominus V_i \ominus A_i \ominus (C_i, E_i)$  form a Markov chain.

We also define an independent random variable  $Q$  uniformly distributed over the set  $\{1, \dots, n\}$ , and  $A = A_Q$ ,  $C = C_Q$ ,  $E = E_Q$ ,  $U = (Q, U_Q)$ , and  $V = (Q, V_Q)$ .  $U \ominus V \ominus A \ominus (C, E)$  still form a Markov chain and  $(A, C, E)$  is distributed according to the joint distribution  $p(a, c, e)$  *i.e.*, the original distribution of  $(A_i, C_i, E_i)$ .

#### A. Rate

$$\begin{aligned} n(R_A + \varepsilon) &\geq H(J) \\ &\stackrel{(a)}{=} I(J; A^n C^n E^n) \\ &\stackrel{(b)}{\geq} I(J; A^n E^n | C^n) \\ &\stackrel{(c)}{=} \sum_{i=1}^n I(J; A_i E_i | A^{i-1} C^n E^{i-1}) \\ &= \sum_{i=1}^n \left[ I(J A^{i-1} C^{i-1} C_{i+1}^n E^{i-1}; A_i E_i | C_i) - I(A^{i-1} C^{i-1} C_{i+1}^n E^{i-1}; A_i E_i | C_i) \right] \\ &\stackrel{(d)}{=} \sum_{i=1}^n I(J A^{i-1} C^{i-1} C_{i+1}^n E^{i-1}; A_i E_i | C_i) \\ &\stackrel{(e)}{\geq} \sum_{i=1}^n I(V_i; A_i | C_i) , \end{aligned}$$

where

- step (a) follows from  $J = f(A^n)$ ,
- step (b) from the non-negativity of mutual information,
- step (c) from the chain rule for conditional mutual information,
- step (d) from the fact that random variables  $A_i$ ,  $C_i$  and  $E_i$  are independent across time,
- step (e) from the non-negativity of mutual information and definition (35).

Then, using random variable  $Q$ ,

$$\begin{aligned} R_A + \varepsilon &\geq \frac{1}{n} \sum_{i=1}^n I(V_Q; A_Q | C_Q, Q = i) \\ &= I(V_Q; A_Q | C_Q Q) \\ &= I(V; A | C) . \end{aligned}$$

### B. Distortion at Bob

Bob reconstructs  $g(J, C^n)$ . For each  $i \in \{1, \dots, n\}$ , define function  $\hat{A}_i$  as the  $i$ -th coordinate of this estimate:

$$\hat{A}_i(V_i, C_i) \triangleq g_i(J, C^{i-1}, C_i, C_{i+1}^n) .$$

The component-wise mean distortion at Bob thus verifies

$$\begin{aligned} D + \varepsilon &\geq \mathbb{E} [d(A^n, g(J, C^n))] \\ &= \frac{1}{n} \sum_{i=1}^n \mathbb{E} [d(A_i, \hat{A}_i(V_i, C_i))] \\ &= \frac{1}{n} \sum_{i=1}^n \mathbb{E} [d(A_Q, \hat{A}_Q(V_Q, C_Q)) \mid Q = i] \\ &= \mathbb{E} [d(A_Q, \hat{A}_Q(V_Q, C_Q))] \\ &= \mathbb{E} [d(A, \hat{A}(V, C))] , \end{aligned}$$

where we defined function  $\hat{A}$  on  $\mathcal{V} \times \mathcal{C}$  by

$$\hat{A}(V, C) = \hat{A}(Q, V_Q, C_Q) \triangleq \hat{A}_Q(V_Q, C_Q) .$$

### C. Equivocation Rate at Eve

$$\begin{aligned}
n(\Delta - \varepsilon) &\leq H(A^n|J, E^n) \\
&= H(A^n|J) - I(A^n; E^n|J) \\
&= H(A^n|JC^n) + I(A^n; C^n|J) - I(A^n; E^n|J) \\
&\stackrel{(a)}{=} H(A^n|JC^n) + I(A^n; C^n) - I(J; C^n) - I(A^n; E^n) + I(J; E^n) \\
&\stackrel{(b)}{=} \sum_{i=1}^n \left[ H(A_i|JA^{i-1}C^n) + I(A_i; C_i) - I(JC_{i+1}^n; C_i) - I(A_i; E_i) + I(JE^{i-1}; E_i) \right] \\
&\stackrel{(c)}{=} \sum_{i=1}^n \left[ H(A_i|JA^{i-1}C^nE^{i-1}) + I(A_i; C_i) - I(JC_{i+1}^n; C_i) - I(A_i; E_i) \right. \\
&\quad \left. + I(JE^{i-1}; E_i) + I(E_i; C_{i+1}^n|JE^{i-1}) - I(C_i; E^{i-1}|JC_{i+1}^n) \right] \\
&= \sum_{i=1}^n \left[ H(A_i|JA^{i-1}C^nE^{i-1}) + I(A_i; C_i) - I(A_i; E_i) \right. \\
&\quad \left. + I(E_i; JC_{i+1}^nE^{i-1}) - I(C_i; JC_{i+1}^nE^{i-1}) \right] \\
&\stackrel{(d)}{=} \sum_{i=1}^n \left[ H(A_i|V_iC_i) + I(A_i; C_i) - I(A_i; E_i) + I(E_i; U_i) - I(C_i; U_i) \right] \\
&\stackrel{(e)}{=} \sum_{i=1}^n \left[ H(A_i|V_iC_i) + I(A_i; C_i|U_i) - I(A_i; E_i|U_i) \right],
\end{aligned}$$

where

- step (a) follows from the Markov chain  $J \multimap A^n \multimap (C^n, E^n)$ ,
- step (b) from the chain rules for conditional entropy and mutual information, and the fact that random variables  $A_i$ ,  $C_i$  and  $E_i$  are independent across time,
- step (c) from the Markov chain  $(A_i, C^i) \multimap (JA^{i-1}) \multimap (C^{i-1}, E^{i-1})$  (see Fig. 16a) and Csiszár and Körner's equality [28] (see Appendix A-C),
- step (d) from definitions (34) and (35),
- step (e) from the Markov chain  $U_i \multimap A_i \multimap (C_i, E_i)$ .



Using auxiliary random variable  $Q$ , this yields

$$\begin{aligned}\Delta - \varepsilon &\leq \frac{1}{n} \sum_{i=1}^n \left[ H(A_Q | V_Q C_Q, Q = i) \right. \\ &\quad \left. + I(A_Q; C_Q | U_Q, Q = i) - I(A_Q; E_Q | U_Q, Q = i) \right] \\ &= H(A | VC) + I(A; C | U) - I(A; E | U) .\end{aligned}$$

#### D. End of Proof

We proved that, for each achievable tuple  $(R_A, D, \Delta)$  and each  $\varepsilon > 0$ , there exist random variables  $U, V$  such that  $U \dashv\vdash V \dashv\vdash A \dashv\vdash (C, E)$  forms a Markov chain, and

$$\begin{aligned}R_A + \varepsilon &\geq I(V; A | C) , \\ D + \varepsilon &\geq \mathbb{E}[d(A, \hat{A}(V, C))] , \\ \Delta - \varepsilon &\leq H(A | VC) + I(A; C | U) - I(A; E | U) .\end{aligned}$$

Recalling that region  $\mathcal{R}_{\text{uncoded}}^*$  is closed, and letting  $\varepsilon$  tend to zero prove the converse part of Theorem 3. ■

## APPENDIX F

### PROOF OF THE CONVERSE PART OF THEOREM 4

Let  $(R_A, R_C, \Delta)$  be an achievable tuple and  $\varepsilon > 0$ . There exists an  $(n, R_A + \varepsilon, R_C + \varepsilon)$ -code  $(f_A, f_C, g)$  s.t.:

$$\begin{aligned}\Pr \{g(f_A(A^n), f_C(C^n)) \neq (A^n, C^n)\} &\leq \varepsilon , \\ \frac{1}{n} H(A^n | f_A(A^n), E^n) &\geq \Delta - \varepsilon .\end{aligned}$$

Denote by  $J = f_A(A^n)$  and  $K = f_C(C^n)$  the messages transmitted by Alice and Charlie, respectively. For each  $i \in \{1, \dots, n\}$ , define random variable  $U_i$  by

$$U_i = (J, C_{i+1}^n, E^{i-1}) . \tag{36}$$

From Fig. 16a,  $U_i \dashv\vdash A_i \dashv\vdash (C_i, E_i)$  form a Markov chain.

We also define an independent random variable  $Q$  uniformly distributed over the set  $\{1, \dots, n\}$ , and  $A = A_Q, C = C_Q, E = E_Q, U = (Q, U_Q)$ . Note that  $U \dashv\vdash A \dashv\vdash (C, E)$  still form a Markov chain, and that  $(A, C, E)$  is distributed according to the joint distribution  $p(a, c, e)$  i.e., the original distribution of  $(A_i, C_i, E_i)$ .

### A. Rate at Alice

Following the argument of the converse for the Slepian-Wolf theorem [53, Section 15.4.2], we prove lower bounds on the rates:

$$\begin{aligned}
 n(R_A + \varepsilon) &\geq H(J) \\
 &\stackrel{(a)}{\geq} H(J|C^n) \\
 &\stackrel{(b)}{=} I(A^n; J|C^n) \\
 &\stackrel{(c)}{=} H(A^n|C^n) - H(A^n|JKC^n) \\
 &\stackrel{(d)}{\geq} nH(A|C) - nO(\varepsilon) ,
 \end{aligned}$$

where

- step (a) follows from the fact that conditioning reduces the entropy,
- step (b) from  $J = f_A(A^n)$ ,
- step (c) from  $K = f_C(C^n)$ ,
- step (d) from the fact that random variables  $A_i$  and  $C_i$  are i.i.d., and Fano's inequality<sup>4</sup>.

### B. Rate at Charlie

Using similar arguments with  $K = f_C(C^n)$ , we can obtain:

$$\begin{aligned}
 n(R_C + \varepsilon) &\geq H(K) \\
 &\stackrel{(a)}{\geq} H(K|J) \\
 &\stackrel{(b)}{=} I(K; C^n|J) \\
 &= H(C^n|J) - H(C^n|JK) \\
 &\stackrel{(c)}{\geq} \sum_{i=1}^n H(C_i|JC_{i+1}^n) - nO(\varepsilon) \\
 &\stackrel{(d)}{\geq} \sum_{i=1}^n H(C_i|U_i) - nO(\varepsilon) ,
 \end{aligned}$$

where

- step (a) follows from the fact that conditioning reduces the entropy,

<sup>4</sup>Landau-like notation  $O(\varepsilon)$  stands for a term  $X$  such that  $0 \leq X \leq k\varepsilon$  for some constant  $k > 0$ .

- step (b) from  $K = f_C(C^n)$ ,
- step (c) from the chain rule for conditional entropy and Fano's inequality,
- step (d) from the fact that conditioning reduces the entropy, and definition (36).

Now, using auxiliary random variable  $Q$ ,

$$\begin{aligned} R_C + \varepsilon &\geq \frac{1}{n} \sum_{i=1}^n H(C_Q|U_Q, Q=i) - O(\varepsilon) \\ &= H(C|U) - O(\varepsilon) . \end{aligned} \tag{37}$$

### C. Sum-rate

A lower bound on the sum-rate can be derived as well:

$$\begin{aligned} n(R_A + R_C + 2\varepsilon) &\geq H(JK) \\ &\stackrel{(a)}{=} I(A^n C^n; JK) \\ &\stackrel{(b)}{\geq} nH(AC) - nO(\varepsilon) , \end{aligned}$$

where

- step (a) follows from  $J = f_A(A^n)$  and  $K = f_C(C^n)$ ,
- step (b) from the fact that random variables  $A_i$  and  $C_i$  are i.i.d., and Fano's inequality.

#### D. Equivocation rate at Eve

$$\begin{aligned}
n(\Delta - \varepsilon) &\leq H(A^n | JE^n) \\
&= H(A^n | J) - I(A^n; E^n | J) \\
&= H(A^n | JK) + I(A^n; K | J) - I(A^n; E^n | J) \\
&\stackrel{(a)}{\leq} nO(\varepsilon) + I(A^n; C^n | J) - I(A^n; E^n | J) \\
&\stackrel{(b)}{=} nO(\varepsilon) + I(A^n; C^n) - I(J; C^n) - I(A^n; E^n) + I(J; E^n) \\
&\stackrel{(c)}{=} nO(\varepsilon) + \sum_{i=1}^n \left[ I(A_i; C_i) - I(JC_{i+1}^n; C_i) - I(A_i; E_i) + I(JE^{i-1}; E_i) \right] \\
&\stackrel{(d)}{=} nO(\varepsilon) + \sum_{i=1}^n \left[ I(A_i; C_i) - I(JC_{i+1}^n; C_i) - I(A_i; E_i) + I(JE^{i-1}; E_i) \right. \\
&\quad \left. + I(E_i; C_{i+1}^n | JE^{i-1}) - I(C_i; E^{i-1} | JC_{i+1}^n) \right] \\
&= nO(\varepsilon) + \sum_{i=1}^n \left[ I(A_i; C_i) - I(JC_{i+1}^n E^{i-1}; C_i) - I(A_i; E_i) + I(JC_{i+1}^n E^{i-1}; E_i) \right] \\
&\stackrel{(e)}{=} nO(\varepsilon) + \sum_{i=1}^n \left[ I(A_i; C_i | U_i) - I(A_i; E_i | U_i) \right],
\end{aligned}$$

where

- step (a) follows from Fano's inequality, and  $K = f_C(C^n)$ ,
- step (b) from the Markov chain  $J \multimap A^n \multimap (C^n, E^n)$ ,
- step (c) from the chain rule for mutual information, and the fact that random variables  $A_i$ ,  $C_i$ , and  $E_i$  are independent across time,
- step (d) from Csiszár and Körner's equality [28] (see Appendix A-C),
- step (e) from definition (36), and the Markov chain  $U_i \multimap A_i \multimap (C_i, E_i)$ .

Now, using auxiliary random variable  $Q$ ,

$$\begin{aligned}
\Delta - \varepsilon &\leq \frac{1}{n} \sum_{i=1}^n \left[ I(A_Q; C_Q | U_Q, Q = i) - I(A_Q; E_Q | U_Q, Q = i) \right] + O(\varepsilon) \\
&= I(A; C | U) - I(A; E | U) + O(\varepsilon).
\end{aligned}$$

### E. End of Proof

We proved that, for each achievable tuple  $(R_A, R_C, \Delta)$  and each  $\varepsilon > 0$ , there exists a random variable  $U$  such that  $U \text{---} A \text{---} (C, E)$  form a Markov chain, and

$$\begin{aligned} R_A + O(\varepsilon) &\geq H(A|C) , \\ R_C + O(\varepsilon) &\geq H(C|U) , \\ R_A + R_C + O(\varepsilon) &\geq H(AC) , \\ \Delta - O(\varepsilon) &\leq I(A; C|U) - I(A; E|U) . \end{aligned}$$

Recalling that region  $\mathcal{R}_{\text{lossless}}^*$  is closed, and letting  $\varepsilon$  tend to zero prove the converse part of Theorem 4. ■

## APPENDIX G

### PROOF OF THE CONVERSE PART OF PROPOSITION 4

The proof of the converse part of Proposition 4 follows the same argument that Appendix F. In particular, definition (36) remains the same. The only difference lies in the lower bound for the rate at Alice:

$$\begin{aligned} n(R_A + \varepsilon) &\geq H(J) \\ &\stackrel{(a)}{=} I(J; A^n|C^n) + I(J; C^n) \\ &\stackrel{(b)}{=} H(A^n|C^n) - H(A^n|JKC^n) + I(J; C^n) \\ &\stackrel{(c)}{\geq} -nO(\varepsilon) + \sum_{i=1}^n \left[ H(A_i|C_i) + I(JC_{i+1}^n; C_i) \right] \\ &\stackrel{(d)}{=} -nO(\varepsilon) + \sum_{i=1}^n \left[ H(A_i|C_i) + I(JC_{i+1}^n; C_i) \right. \\ &\quad \left. + I(E^{i-1}; C_i|JC_{i+1}^n) - I(C_{i+1}^n; E_i|JE^{i-1}) \right] \\ &\stackrel{(e)}{\geq} -nO(\varepsilon) + \left[ \sum_{i=1}^n H(A_i|C_i) + I(JC_{i+1}^n E^{i-1}; C_i) - I(JC_{i+1}^n E^{i-1}; E_i) \right] \\ &\stackrel{(f)}{=} -nO(\varepsilon) + \sum_{i=1}^n \left[ H(A_i|C_i) + I(U_i; C_i) - I(U_i; E_i) \right] , \end{aligned}$$

where

- step (a) follows from  $J = f_A(A^n)$ ,
- step (b) from  $K = f_C(C^n)$ ,
- step (c) from Fano's inequality, the chain rule for conditional mutual information and the fact that random variables  $A_i, C_i$  are independent across time,
- step (d) from Csiszár and Körner's equality [28],
- step (e) from the fact that random variables  $A_i, C_i$  and  $E_i$  are independent across time, and the non-negativity of mutual information,
- step (f) from definition (36).

Using random variable  $Q$  and following the argument of Appendix F, we proved the following lower bound:

$$R_A + \varepsilon \geq H(A|C) + I(U; C) - I(U; E) - O(\varepsilon) .$$

Since Equation (37) still holds, we proved the bound on  $R_A$  given by Proposition 4. Other steps of the proof remain unchanged. ■

#### ACKNOWLEDGMENT

The authors are grateful to Prof. Shlomo Shamai (Shitz) for many helpful discussions.

#### REFERENCES

- [1] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, 1973.
- [2] A. Wyner, "On source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 21, no. 3, pp. 294–300, 1975.
- [3] R. Ahlswede and J. Körner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Inf. Theory*, vol. 21, no. 6, pp. 629–637, 1975.
- [4] T. Berger, *Multiterminal source coding*. Springer-Verlag, 1977.
- [5] T. Berger, K. Housewright, J. Omura, S. Yung, and J. Wolfowitz, "An upper bound on the rate distortion function for source coding with partial side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 25, no. 6, pp. 664–666, 1979.
- [6] S. Jana and R. Blahut, "Partial side information problem: Equivalence of two inner bounds," in *Proc. CISS*, 2008, pp. 1005–1009.
- [7] A. Wagner, B. Kelly, and Y. Altug, "The lossy one-helper conjecture is false," in *Proc. Allerton*, 2009, pp. 716–723.
- [8] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, 1976.
- [9] T. Berger and R. Yeung, "Multiterminal source encoding with one distortion criterion," *IEEE Trans. Inf. Theory*, vol. 35, no. 2, pp. 228–236, 1989.

- [10] Y. Oohama, "Gaussian multiterminal source coding," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1912–1923, 1997.
- [11] A. Wagner, S. Tavildar, and P. Viswanath, "Rate region of the quadratic Gaussian two-encoder source-coding problem," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1938–1961, 2008.
- [12] T. Han and K. Kobayashi, "A unified achievable rate region for a general class of multiterminal source coding systems," *IEEE Trans. Inf. Theory*, vol. 26, no. 3, pp. 277–288, 1980.
- [13] I. Csiszar and J. Korner, "Towards a general theory of source networks," *IEEE Trans. Inf. Theory*, vol. 26, no. 2, pp. 155–165, 1980.
- [14] C. Heegard and T. Berger, "Rate distortion when side information may be absent," *IEEE Trans. Inf. Theory*, vol. 31, no. 6, pp. 727–734, 1985.
- [15] A. Kaspi, "Rate-distortion function when side-information may be present at the decoder," *IEEE Trans. Inf. Theory*, vol. 40, no. 6, pp. 2031–2034, 1994.
- [16] A. Kaspi and T. Berger, "Rate-distortion for correlated sources with partially separated encoders," *IEEE Trans. Inf. Theory*, vol. 28, no. 6, pp. 828–840, 1982.
- [17] C. Tian and S. Diggavi, "On multistage successive refinement for Wyner–Ziv source coding with degraded side informations," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2946–2960, 2007.
- [18] —, "Side-information scalable source coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5591–5608, 2008.
- [19] R. Timo, T. Chan, and A. Grant, "Rate distortion with side-information at many decoders," *arXiv cs.IT*, vol. 0901.1705, pp. 1–36, 2010.
- [20] S. Tavildar, P. Viswanath, and A. Wagner, "The Gaussian many-help-one distributed source coding problem," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 564–581, 2010.
- [21] M. Rahman and A. Wagner, "Rate region of the Gaussian scalar-help-vector source-coding problem," in *Proc. ISIT*, 2010, pp. 56–60.
- [22] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250–1276, 2002.
- [23] A. Liveris, Z. Xiong, and C. Georgiades, "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Commun. Lett.*, vol. 6, no. 10, pp. 440–442, 2002.
- [24] S. Servetto, "Lattice quantization with side information: Codes, asymptotics, and applications in sensor networks," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 714–731, 2007.
- [25] S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): design and construction," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 626–643, 2003.
- [26] C. Shannon, "Communication theory of secrecy systems," *BSTJ*, vol. 28, pp. 656–715, 1949.
- [27] A. Wyner, "The wire-tap channel," *BSTJ*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [28] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [29] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.
- [30] M. Bloch and J. Laneman, "On the secrecy capacity of arbitrary wiretap channels," in *Proc. Allerton*, 2008, pp. 818–825.
- [31] Y. Chen and A. Han Vinck, "Wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 395–402, 2008.

- [32] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, 2011.
- [33] "Special issue on information theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2405–2818, 2008.
- [34] Y. Liang, H. Poor, and S. Shamai, *Information theoretic security*. Now Publishers, 2009.
- [35] R. Liu and W. Trappe, *Securing wireless communications at the physical layer*. Springer, 2010.
- [36] R. Liu, Y. Liang, H. Poor, and P. Spasojevic, "Secure nested codes for type II wiretap channels," in *Proc. ITW*, 2007, pp. 337–342.
- [37] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," in *Proc. ITW*, 2009, pp. 95–99.
- [38] F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: Construction and analysis," *arXiv cs.IT*, vol. 1103.4086, pp. 1–40, 2011.
- [39] H. Mahdavi and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," in *Proc. ISIT*, 2010, pp. 913–917.
- [40] M. Hayashi and R. Matsumoto, "Construction of wiretap codes from ordinary channel codes," in *Proc. ISIT*, 2010, pp. 2538–2542.
- [41] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography—Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.
- [42] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.
- [43] H. Yamamoto, "A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers," *IEEE Trans. Inf. Theory*, vol. 29, no. 6, pp. 918–923, 1983.
- [44] —, "A rate-distortion problem for a communication system with a secondary decoder to be hindered," *IEEE Trans. Inf. Theory*, vol. 34, no. 4, pp. 835–842, 1988.
- [45] —, "Coding theorems for Shannon's cipher system with correlated source outputs, and common information," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 85–95, 1994.
- [46] —, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 827–835, 1997.
- [47] N. Merhav, "On the Shannon cipher system with a capacity-limited key-distribution channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1269–1273, 2006.
- [48] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," in *Proc. ITW*, 2007, pp. 442–447.
- [49] D. Gunduz, E. Erkip, and H. Poor, "Secure lossless compression with side information," in *Proc. ITW*, 2008, pp. 169–173.
- [50] R. Tandon, S. Ulukus, and K. Ramchandran, "Secure source coding with a helper," in *Proc. Allerton*, 2009, pp. 1061–1068.
- [51] D. Gunduz, E. Erkip, and H. Poor, "Lossless compression with security constraints," in *Proc. ISIT*, 2008, pp. 111–115.
- [52] A. El Gamal and Y.-H. Kim, *Lecture Notes on Network Information Theory*, arXiv:1001.3404, 2010.
- [53] T. Cover and J. Thomas, *Elements of information theory (2nd Ed)*. Wiley-Interscience, 2006.
- [54] C. Nair, "Capacity regions of two new classes of two-receiver broadcast channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4207–4214, 2010.
- [55] A. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications—Part I," *IEEE Trans. Inf. Theory*, vol. 19, no. 6, pp. 769–772, 1973.
- [56] T. Liu and P. Viswanath, "An extremal inequality motivated by multiterminal information-theoretic problems," *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1839–1851, 2007.



- [57] O. Rioul, “Information theoretic proofs of entropy power inequalities,” *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 33–55, 2011.
- [58] Y. Oohama, “Rate-distortion theory for Gaussian multiterminal source coding systems with several side informations at the decoder,” *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2577–2593, 2005.
- [59] T. Flynn and R. Gray, “Encoding of correlated observations,” *IEEE Trans. Inf. Theory*, vol. 33, no. 6, pp. 773–787, 1987.
- [60] T. Berger, Z. Zhang, and H. Viswanathan, “The CEO problem,” *IEEE Trans. Inf. Theory*, vol. 42, no. 3, pp. 887–902, 1996.
- [61] J. Chen and T. Berger, “Successive Wyner–Ziv coding scheme and its application to the quadratic Gaussian CEO problem,” *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1586–1603, 2008.
- [62] Y. Oohama, “The rate-distortion function for the quadratic Gaussian CEO problem,” *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 1057–1070, 1998.
- [63] I. Csiszar and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Akadémiai Kiado, Budapest, 1982.
- [64] H. Permuter, Y. Steinberg, and T. Weissman, “Two-way source coding with a helper,” *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2905–2919, 2010.
- [65] J. Pearl, “Fusion, propagation, and structuring in belief networks,” *Artificial intelligence*, vol. 29, no. 3, pp. 241–288, 1986.
- [66] G. Kramer, “Capacity results for the discrete memoryless network,” *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 4–21, 2003.
- [67] J. Villard and P. Piantanida, “Secure lossy source coding with side information at the decoders,” in *Proc. Allerton*, 2010.
- [68] —, “Secure distributed lossless compression with side information at the eavesdropper,” in *Proc. Securenets*, 2011.